Cusps, Congruence Groups and Monstrous Dessins

Valdo Tatitscheff[1,2,3] Yang-Hui He[2,4,5] John McKay[6]

[1] Department of Mathematics, Ecole Normale Supérieure, Paris 75005, France
[2] Department of Mathematics, City, University of London, EC1V 0HB, UK
[3] IRMA, UMR 7501, Université de Strasbourg et CNRS,
7, rue René Descartes, 67000 Strasbourg, France
[4] Merton College, University of Oxford, OX14JD, UK
[5] School of Physics, NanKai University, Tianjin, 300071, P.R. China
[6] Department of Mathematics and Statistics,
Concordia University, 1455 de Maisonneuve Blvd. West,
Montreal, Quebec, H3G 1M8, Canada

valdo.tatitscheff@normalesup.org
hey@maths.ox.ac.uk
mckay@encs.concordia.ca

Abstract

We study general properties of the dessins d'enfants associated with the Hecke congruence subgroups $\Gamma_0(N)$ of the modular group $\mathrm{PSL}_2(\mathbb{Z})$. The definition of the $\Gamma_0(N)$ as the stabilisers of couples of projective lattices in a two-dimensional vector space gives an interpretation of the quotient set $\Gamma_0(N)\backslash\mathrm{PSL}_2(\mathbb{Z})$ as the projective lattices N-hyperdistant from a reference one, and hence as the projective line over the ring $\mathbb{Z}/N\mathbb{Z}$. The natural action of $\mathrm{PSL}_2(\mathbb{Z})$ on the lattices defines a dessin d'enfant structure, allowing for a combinatorial approach to features of the classical modular curves, such as the torsion points and the cusps. We tabulate the dessins d'enfants associated with the 15 Hecke congruence subgroups of genus zero, which arise in Moonshine for the Monster sporadic group.

Introduction and motivations

Monstrous moonshine

The vast subject of Moonshine began with the third author's observation, initially thought to be outlandish, that

$$196,884 = 196,883 + 1 \ . \tag{1}$$

The number on the left is the linear Fourier coefficient of the Klein J-function, and lives in the world of modular forms, while the number on the right comes from the first two irreducible representations of the Monster sporadic group $\mathbb{M}$, and lives in the world of finite group theory. These two fields are seemingly disparate.

Based on the observation in Equation 1 and generalisations of it, Thompson conjectured in [Tho79] that there exists a natural graded infinite-dimensional representation $W^\natural = \bigoplus_{n=-1}^{\infty} W_n^\natural$ of $\mathbb{M}$, such that $(\dim(W_n^\natural))_n$ is the sequence of Fourrier coefficients of Klein's J-function, and Atkin, Fong and Smith verified that such an $\mathbb{M}$-module exists [Smi85]. The construction of this module was later given in [FLM89] by Frenkel, Lepowsky and Meurman, thus proving Thompson's conjecture.

The latter had also further suggested to investigate the properties of the graded-traced functions now called **McKay-Thompson series**

$$T_{\bar{g}}(q) = q^{-1} \sum_{k=0}^{\infty} \mathrm{ch}_{W_k^\natural}(\bar{g}) q^k = q^{-1} + 0 + h_1(\bar{g})q + h_2(\bar{g})q^2 + \dots \ ,$$

where $\mathrm{ch}_{W_k^\natural}(\bar{g})$ denotes the character of the representation $W_k^\natural$ of $\mathbb{M}$, evaluated on the conjugacy class $\bar{g}$. This ultimately prompted the Monstrous Moonshine conjectures of [CN79]: each McKay-Thompson series $T_{\bar{g}}(q)$ corresponding to a conjugacy class $\bar{g}$ in $\mathbb{M}$ is, for $q = \exp(2\pi i z)$, the (normalised) generator of a *genus zero function field* for a group G between the Hecke group $\Gamma_0(N)$ of level N and its normaliser $\Gamma_0(N)^+$ in $PSL(2,\mathbb{R})$, generated by $\Gamma_0(N)$ and certain Atkin-Lehner involutions [AL70]. Moreover, the level N is a multiple of $n = \mathrm{Order}(\bar{g})$, the ratio $N/n = h \in \mathbb{Z}_{>0}$ divides 24, and h^2 divides N. In particular, for the conjugacy class of the identity the McKay-Thompson series is the Fourier expansion of the J-function. The latter generates the function field of the genus zero quotient of the Poincaré half-plane by the modular group $\mathrm{PSL}_2(\mathbb{Z})$.

Borcherds proved these conjectures in [Bor92], using in a central way the monster module constructed by Frenkel, Lepowsky and Meurman.

There are 194 conjugacy classes (and hence 194 irreducible representations) of $\mathbb{M}$ (see [CCN$^+$03]) and due to complex conjugation they give only 172 distinct McKay-Thompson series (which are not independent: linear relations brings the number of independent series down to 163). Each of these 172 conjugacy classes corresponds to a group $G_{\bar{g}}$ which lies (strictly,for most of them) between $\Gamma_0(N)$ and $\Gamma_0(N)^+$. Precisely 15 correspond to the Hecke groups of our concern (and do not involve Atkin-Lehner involutions).

Each group $G_{\bar{g}}$ is a subgroup of $\mathrm{PSL}_2(\mathbb{R})$, hence it defines a complex surface: the quotient of the upper half-plane $\mathbb{H}$ by $G_{\bar{g}}$. This complex surface is always of genus 0, has hyperbolic cusps and may have torsion points. The tabulation of the conjugacy classes of the Monster, together with quantities related to them through the moonshine

correspondence (such as the number of cusps of the corresponding modular curve), is given in [CN79].

For more details on the Monstrous Moonshine programme, see the excellent accounts [Gan06, DGO15].

Cusps and exceptional Lie algebras

The motivation for this work essentially comes from some observations listed in [HM15], which let one hope for some links between the three biggest sporadic finite simple groups (the monster group $\mathbb{M}$, the baby monster $\mathbb{B}$ and Fischer's sporadic group Fi'_{24}), and the three biggest exceptional Lie algebras (E_8, E_7 and E_6). While the purpose of this paper is not to address such possible correspondences, and is dedicated to the exposition of a new approach to some properties of the Hecke groups from a purely combinatorial point of view, let us nevertheless review briefly those intriguing epiphanies.

The most famous observation (that we will leave aside) is known as *McKay's monstrous E_8 observation* (see [Con85], §14). The conjugacy classes of the monster group are conventionally labeled with a number and a letter, where the number is the order of the elements in this class and the letter, a label which distinguishes the different classes with that order. In particular, there are two conjugacy classes of order 2, denoted $2A$ and $2B$. Multiplying two elements of the class $2A$ yields an element which is in one of the conjugacy classes $1A, 2A, 2B, 3A, 3C, 4A, 4B, 5A$ or $6A$. The third author noticed a striking correspondence between this sequence and the extended E_8 diagram. The same type of phenomenon happens between the elements of the pairs $(\mathbb{B}, E_7)$ and (Fi_{24}, E_6).

The number of *cusps* of the modular curves corresponding to the conjugacy classes in $\mathbb{M}$ is either 1, 2, 3, 4, 6 or 8. The total number of cusps of the modular curves appearing in the monstrous moonshine correspondence for the group $\mathbb{M}$ (respectively, $2\mathbb{B}$, and $3Fi_{24}$ which are subgroups of $\mathbb{M}$) is $360 = 3 \times 120$ (respectively, $448 = 2^3 \times 56$, and $440 = 2^3(2 \times 27 + 1)$). The exceptional Lie algebra $\mathfrak{e}_8$ has 120 positive roots (respectively, 56 is the dimension of the smallest fundamental representation of $\mathfrak{e}_7$, and 27 is the dimension of the adjoint representation of $\mathfrak{e}_6$). Any relationship between sporadic groups and exceptional Lie algebras would be quite amazing, and thus we are eyeing a better understanding of the cusps of those modular surfaces.

The *coincidence* that directly motivates this article concerns the Hecke congruence subgroups of $\mathrm{PSL}_2(\mathbb{Z})$, which are denoted $\Gamma_0(N)$. These define special modular curves called the *classical modular curves* (and denoted $X_0(N)$). Those of genus zero all appear in the monstrous moonshine correspondence as linked to conjugacy classes in $\mathbb{M}$. It is known that among the $X_0(N)$, 15 of them exactly have genus 0, namely when

$$N \in \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12, 13, 16, 18, 25\} =: I_0 \ .$$

Let $c(N)$ denote the number of cusps of $X_0(N)$. Then:

$$\sum_{N \in I_0} c(N) = 56 \ ,$$

$$\sum_{N\in I_0} c(N)^2 = 266 = 2\times 133\ .$$

The two numbers 56 and 133 are respectively the dimensions of the smallest fundamental representation and of the adjoint representation of the exceptional Lie algebra $\mathfrak{e}_7$. The relationship between the set of cusps of the Hecke subgroups of genus zero and $\mathfrak{e}_7$ still remains to be established, if any.

The approach developed in this paper (initially thought as an auxiliairy way to define the cusps of the Hecke groups) yields a nice combinatorial framework to study the classical modular curves. There is no need for complex geometry nor elliptic elements of $\mathrm{PSL}_2(\mathbb{R})$ in order to define and study the cusps of the Hecke groups - complex geometry only appears as one speaks of Hauptmoduln, such as Klein's invariant J. If the Lie algebras are supposed to connect with monstrous moonshine through the cusps of the modular curves, this simpler framework may be of some interest.

Summary and plan

The cornerstone of what follows is Conway's approach to arithmetic groups in terms of their action on projective lattices in a real vector space [Con96]. Because we are mainly following the introduction to these ideas given in [Dun09], moreover presented in details (in the specific framework we are interested in) in Appendix A, we get to the heart of the matter as directly as possible.

Section 1 aims at a combinatorial description of the quotient set $\Gamma_0(N)\backslash\mathrm{PSL}_2(\mathbb{Z})$. This set is naturally identified with the set $\mathrm{P}\mathcal{L}_1^N$ of projective lattices N-hyperdistant from a reference L_1, which is itself in bijection with $\mathbb{P}^1(\mathbb{Z}/N\mathbb{Z})$, the projective line over the ring $\mathbb{Z}/N\mathbb{Z}$. The resulting bijection

$$\Gamma_0(N)\backslash\mathrm{PSL}_2(\mathbb{Z}) \simeq \mathbb{P}^1(\mathbb{Z}/N\mathbb{Z}) \tag{2}$$

becomes very interesting as one studies the right action of $\mathrm{PSL}_2(\mathbb{Z})$ on $\Gamma_0(N)\backslash\mathrm{PSL}_2(\mathbb{Z})$. The projective line indeed has homogeneous coordinates, in terms of which the right action of $\mathrm{PSL}_2(\mathbb{Z})$ takes a pretty guise. The bijection in Equation 2 is elementary and known since long - it appears for example in [Man72]; the derivation given below however has the advantage of being elementary and quite straightforward, the third description of this set as a set of projective lattices being of great help. Conversely, homogeneous coordinates on $\mathbb{P}^1(\mathbb{Z}/N\mathbb{Z})$ provide coordinates on $\mathrm{P}\mathcal{L}_1^N$, which can thus be described in details.

In section 2 we first review some general features of Grothendieck's dessins d'enfants, and then investigate some of the properties of the special dessins associated with the $\Gamma_0(N)$. The set of edges of the latter is naturally in bijection with $\Gamma_0(N)\backslash\Gamma_0(1) \simeq \mathcal{L}_1^N \simeq \mathbb{P}^1(\mathbb{Z}/N\mathbb{Z})$. Homogeneous coordinates on the projective line provide an algorithmic way to compute these dessins d'enfants, and hence to understand the structure of the modular curves associated with the $\Gamma_0(N)$.

The number of torsion points, as well as the cusps and their width, are controlled by elementary algebraic equations. These equations are also know since long - they appear for example in §1.6 of [Shi71] or as Prop. 2.2 in [Man72], but our approach seems interesting

per se. We compute the Dirichlet L-series corresponding to the sequence $(c(N))_{N\geq 1}$, and express this series in terms of the Riemann ζ-function. For the sake of completeness, we explain in some details how one goes from our dessins d'enfants associated with the $\Gamma_0(N)$, to the complex modular curves $X_0(N)$. Since explicit rational parametrisations of the genus zero classical modular curves are known, there are explicit expressions of Belyĭ maps which yield the Hecke dessins d'enfants of genus 0, and we tabulate them.

Section 3 displays, for each of the 15 Hecke modular groups of genus 0, a fundamental domain in $\mathbb{H}$, the corresponding dessin d'enfants, and a list of its cusps in terms of projective lattices.

Contents

Nomenclature

- Real segments will be written in a standard way:

$$[a,b],\ ]a,b[,\ ]a,b] \text{ or } [a,b[\ ,$$

  where $a, b \in \mathbb{R} \cup \{\pm\infty\}$, depending on whether they are closed, open, open-closed or closed-open.

- For M and M two integers, $[|M,N|]$ denotes the set of integers between M and N, $[|M,N|[$, the set of integers between M and N excluding N, ...
- The set $\mathrm{Div}(N)$ is the set of positive divisors of a non-zero positive integer N.
- For $k, N \in \mathbb{N}$, k divides N is written $k|N$.
- The group of permutations of a set E is denoted $\mathfrak{S}(E)$.
- If H and G are two groups, $H < G$ means that H is a subgroup of G.

Let now V be a two-dimensional real vector space with basis (e_1, e_2). Lattices in V are by definition the $\mathbb{Z}$-submodules of V isomorphic to $\mathbb{Z}^2$. Since we will also need projective lattices, regular lattices (the ones we just defined) are often referred to as non-projective lattices. Let

$$L_1^{np} = \mathbb{Z} \cdot e_1 + \mathbb{Z} \cdot e_2$$

be the non-projective lattice generated by the vectors of the basis (e_1, e_2). The set $\mathcal{L}$ of non-projective lattices in V is in bijection with with $\mathrm{SL}_2(\mathbb{Z})\backslash\mathrm{GL}_2^+(\mathbb{R})$. A lattice $L^{np} \in \mathcal{L}$ such that $L^{np} \cap L_1^{np}$ has finite index in both L^{np} and L_1^{np} is said to be commensurable with L_1^{np}.

A projective lattice in V is an equivalence class of lattices in V up to (rational or real) scaling. Let L_1 be the projective lattice containing L_1^{np}. Commensurability transposes well to projective lattices. The set $\mathrm{P}\mathcal{L}_1$ of projective lattices commensurable with L_1 is identified with $\mathrm{PSL}_2(\mathbb{Z})\backslash\mathrm{PGL}_2^+(\mathbb{Q})$.

There exists a symmetric function

$$\delta : \mathrm{P}\mathcal{L}_1 \times \mathrm{P}\mathcal{L}_1 \to \mathbb{N}_{>0}$$

called hyperdistance. The right-action of $\mathrm{PSL}_2(\mathbb{Z})$ on $\mathrm{P}\mathcal{L}_1$ preserves the hyperdistance. For any $N \in \mathbb{N}_{>0}$, we let $\mathrm{P}\mathcal{L}_1^N \subset \mathrm{P}\mathcal{L}_1$ denote the set of projective lattices N-hyperdistant from L_1, i.e. the set of projective lattices L such that $\delta(L, L_1) = N$.

The group $G = \mathrm{PGL}_2^+(\mathbb{Q})$ acts on the right of $\mathrm{P}\mathcal{L}_1$, and the modular group $\mathrm{PSL}_2(\mathbb{Z})$ is naturally identified with $\mathrm{Stab}_G(L_1)$.

As shown in Prop. 26, the set $\mathrm{PSL}_2(\mathbb{Z})\backslash\mathrm{PGL}_2^+(\mathbb{Q})$ is identified with the set $\mathcal{M}$ of matrices of the form $\begin{pmatrix} M & b \\ 0 & 1 \end{pmatrix}$, for $M \in \mathbb{Q}_+^*$ and $b \in \mathbb{Q} \cap [0, 1[$. Following [Con96], we write $L_{M,b}$ to refer to the projective lattice commensurable with L_1 corresponding to the class

$$\mathrm{PSL}_2(\mathbb{Z}) \cdot \begin{pmatrix} M & b \\ 0 & 1 \end{pmatrix} \in \mathrm{PSL}_2(\mathbb{Z})\backslash\mathrm{PGL}_2^+(\mathbb{Q}) \ .$$

When $b = 0$, the label $L_{M,b}$ is shortened to L_M.

The Hecke congruence subgroup of level N of the modular group is defined to be $\Gamma_0(N) = \mathrm{Stab}_G(L_1, L_N)$.

In Appendix A more details on this approach to arithmetic groups via their action on lattices are given.

Remark. *Note that although V is the real vector space in which we consider (projective) lattices in order to define and study the modular groups of our interest, V also generically denotes the set of vertices of graphs - and we will stick to this conventional notation. What V stands for in what follows is however always clear from the context, hence we hope that this unfortunate notation conflict will not be too much of a discomfort, while reading.*

1 $\Gamma_0(N)\backslash\Gamma_0(1)$ as the projective line $\mathbb{P}^1(\mathbb{Z}/N\mathbb{Z})$

The goal of this section is to prove that

$$\mathbb{P}^1(\mathbb{Z}/N\mathbb{Z}) \simeq \mathrm{P}\mathcal{L}_1^N \simeq \Gamma_0(N)\backslash\Gamma_0(1) \ , \tag{3}$$

These bijections provide a nice framework to study $\Gamma_0(N)\backslash\Gamma_0(1)$: conceptually, because of the definition of $\mathrm{P}\mathcal{L}_1^N$, as well as in practice, since the homogeneous coordinates on $\mathbb{P}^1(\mathbb{Z}/N\mathbb{Z})$ give an explicit description of $\Gamma_0(N)\backslash\Gamma_0(1)$. We first construct the bijection $\mathbb{P}^1(\mathbb{Z}/N\mathbb{Z}) \leftarrow \mathrm{P}\mathcal{L}_1^N$ and then, the other one: $\mathrm{P}\mathcal{L}_1^N \simeq \Gamma_0(N)\backslash\Gamma_0(1)$. From this one easily computes the index $[\Gamma_0(1) : \Gamma_0(N)]$.

1.1 The bijection $\mathrm{P}\mathcal{L}_1^N \to \mathbb{P}^1(\mathbb{Z}/N\mathbb{Z})$

Let $\tilde{L}^{np}$ be the non-projective lattice commensurable with L_1^{np} corresponding to some coset

$$\mathrm{SL}_2(\mathbb{Z}) \cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})\backslash\mathrm{GL}_2^+(\mathbb{Q}) \ .$$

It is a subgroup of L_1^{np} if and only if $a, b, c, d \in \mathbb{Z}$. The index $N = [L_1^{np} : \tilde{L}^{np}]$ equals $\det \begin{pmatrix} a & b \\ c & d \end{pmatrix} = N$. The order of any element in $L_1^{np}/\tilde{L}^{np}$ divides N, hence

$$N \cdot L_1^{np} \leq \tilde{L}^{np} \leq L_1^{np}$$

For all $n \in \mathbb{N}_{>0}$ let

$$\mathrm{red}_n : \begin{cases} \tilde{L}^{np} & \to & (\mathbb{Z}/n\mathbb{Z})^2 \\ (k\ l)_{\mathrm{ref}} & \mapsto & (\mathrm{red}_n(k), \mathrm{red}_n(l)) \end{cases} \tag{4}$$

be the map of reduction modulo n, where $(k\ l)_{\mathrm{ref}}$ denotes the coordinate expression of a point in $\tilde{L}^{np}$, in the reference basis.

Proposition 1. *The reduction modulo N of the sublattice $\tilde{L}^{np}$ of L_1^{np} of index $N \in \mathbb{N}_{>0}$ is a $\mathbb{Z}/N\mathbb{Z}$-submodule of $(\mathbb{Z}/N\mathbb{Z})^2$, and its cardinality is N.*

Proof. Let (f^1, f^2) be an oriented basis of $\tilde{L}^{np}$, i.e $\tilde{L}^{np} = \mathbb{Z} \cdot f^1 + \mathbb{Z} \cdot f^2$, where the coordinates of the f^i $(i = 1, 2)$ in the reference basis are $(f_1^i\ f_2^i)_{\mathrm{ref}}$. Let $P = p_1 f^1 + p_2 f^2$ with $p_1, p_2 \in \mathbb{Z}$. Then:

$$P = \left(p_1 f_1^1 \ + p_2 f_1^2,\ p_1 f_2^1 \ + p_2 f_2^2\right)_{\mathrm{ref}}$$

Hence $\mathrm{red}_N(P) = \left(\mathrm{red}_N(p_1 f_1^1 \ + p_2 f_1^2), \mathrm{red}_N(\ p_1 f_2^1 \ + p_2 f_2^2)\right)$. Let now $P, Q \in \tilde{L}^{np}$. One readily sees that $\mathrm{red}_N(P + Q) = \mathrm{red}_N(P) + \mathrm{red}_N(Q)$ and hence $\mathrm{red}_N(\tilde{L}^{np})$ is an abelian group. Moreover, the $\mathbb{Z}$-module structure on $\tilde{L}^{np}$ induces a $\mathbb{Z}/N\mathbb{Z}$-module structure on $\mathrm{red}_N(\tilde{L}^{np})$. The index condition implies that $\mathrm{red}_N(\tilde{L}^{np})$ has exactly N elements. □

Definition 1. *The projective line $\mathbb{P}^1(\mathbb{Z}/N\mathbb{Z})$ is the set of $\mathbb{Z}/N\mathbb{Z}$-submodules of $(\mathbb{Z}/N\mathbb{Z})^2$ which are free and of rank 1.*

Proposition 2. *The relation $\sim$ on the pairs $(c, d) \in (\mathbb{Z}/N\mathbb{Z})^2$, such that $(c, d) \sim (c', d')$ if $(c', d') = l \cdot (c, d)$ for some $l \in (\mathbb{Z}/N\mathbb{Z})^\times$, is an equivalence relation.*

The projective line $\mathbb{P}^1(\mathbb{Z}/N\mathbb{Z})$ can be equivalently defined as:

$$\{(a,b) \in (\mathbb{Z}/N\mathbb{Z})^2 | (\mathbb{Z}/N\mathbb{Z}) \cdot a + (\mathbb{Z}/N\mathbb{Z}) \cdot b = (\mathbb{Z}/N\mathbb{Z})\}/\sim \ .$$

Let $[c:d]$ denote the equivalence class of (c,d), modulo $\sim$. Then:

$$\mathbb{P}^1(\mathbb{Z}/N\mathbb{Z}) \simeq \{[a:b] \subset (\mathbb{Z}/N\mathbb{Z})^2/\sim | (\mathbb{Z}/N\mathbb{Z}) \cdot a + (\mathbb{Z}/N\mathbb{Z}) \cdot b = (\mathbb{Z}/N\mathbb{Z})\} \ ,$$

which makes sense since the constraint in the bracket does not depend on the choice of representatives (a,b) for each class $[a:b]$. If one represents $\mathbb{Z}/N\mathbb{Z}$ as $[|0, N-1|]$, the invertibles are:

$$(\mathbb{Z}/N\mathbb{Z})^\times \simeq \{a \in [|0, N-1|] | \gcd(a,N) = 1\} \ .$$

Proposition 3. *The following bijection holds:*

$$\mathbb{P}^1(\mathbb{Z}/N\mathbb{Z}) \simeq \{[c:d] | c,d \in [|0,N-1|]^2, \gcd(c,d,N) = 1\} \ .$$

Proof. First note that the property $\gcd(c,d,N) = 1$ is well-defined modulo N, and because invertibles of $\mathbb{Z}/N\mathbb{Z} = [|0, N-1|]$ are the integers coprime with N, one sees that it is in fact well defined on the equivalence classes $[c:d]$. Now, note that if $x = \gcd(c,d,N) > 1$ then N/x is non-zero and satisfies $(N/x)\cdot c = (N/x)\cdot d = 0$, hence the module $\mathbb{Z}/N\mathbb{Z}\cdot(c,d)$ is not free. Thus there is a map:

$$\mathbb{P}^1(\mathbb{Z}/N\mathbb{Z}) \to \{[c:d] | c,d \in [|0,N-1|]^2, \gcd(c,d,N) = 1\} \ .$$

Conversely, given any representative of $[c:d]$ with $c,d \in [|0,N-1|]$ and $\gcd(c,d,N) = 1$, the module $\mathbb{Z}/N\mathbb{Z}\cdot(c,d)$ is free (otherwise there would be an $a \neq 0$ such that $a\cdot(c,d) = (0,0)$, which would contradict $\gcd(c,d,N) = 1$). These two maps are mutually inverse, and that concludes the proof. □

This result is classical and can for example be found as Proposition 2.4 in [Man72].

Remark 1. *Let $[c:d]$ be the equivalence class of a pair $(c,d) \in [|0,N-1|]^2$ such that $\gcd(c,d) = k$ and $\gcd(k,N) = 1$ i.e. k is invertible. Now, $\gcd(k^{-1}c, k^{-1}d) = 1$, and $[c:d] = [k^{-1}c : k^{-1}d]$. Hence*

$$\mathbb{P}^1(\mathbb{Z}/N\mathbb{Z}) \simeq \{[c:d] | c,d \in [|0,N-1|], \ \gcd(c,d) = 1\}$$

The different representatives $(c',d') \in [|0,N-1|]^2$ of an equivalence class $[c:d]$ such that $\gcd(c,d) = 1$ are exactly the bases of the free module which is the point in $\mathbb{P}^1(\mathbb{Z}/N\mathbb{Z})$ under consideration.

Definition 2. *Let L be a projective lattice in $\mathrm{P}\mathcal{L}_1$, N-hyperdistant from L_1. Among all the non-projective representatives of L some are sub-groups of L_1^{np}. Let L^{np} be the one for which the index $[L_1^{\mathrm{np}} : L^{\mathrm{np}}]$ is minimal (hence equal to N - see Appendix A).*

Proposition 4. *Let L be a projective lattice in $\mathrm{P}\mathcal{L}_1$, N-hyperdistant from L_1. Then $\mathrm{red}_N(L^{\mathrm{np}})$ is a free, rank-1 sub-module of $(\mathbb{Z}/N\mathbb{Z})^2$.*

Proof. We want to show that $\mathrm{red}(L^{\mathrm{np}})$ contains some point $(c,d) \in [|0, N-1|]^2$ with $\gcd(c,d) = 1$. As shown in Appendix A, any projective lattice commensurable with L_1 is an $L_{M,b}$ for some $M \in \mathbb{Q}_+^*$ and $b \in \mathbb{Q} \cap [0,1[$. Let α be the smallest strictly positive integer such that αM and αb are also integers. Hence $\gcd(\alpha M, \alpha b, \alpha) = 1$, $\delta(L_{M,b}, L_1) = N = \alpha^2 M$, and $\alpha b \in [0, \alpha[\cap \mathbb{Z}$.

- If $\alpha M = 1$, the point $v = (1 \ \alpha b)_{\mathrm{ref}} \in L^{\mathrm{np}}$ works.
- If $\alpha M > 1$ and $\gcd(\alpha M, \alpha b) = 1$, the point $v = (\alpha M \ \alpha b)_{\mathrm{ref}} \in L^{\mathrm{np}}$ works.
- If $\alpha M > 1$ and $\gcd(\alpha M, \alpha b) > 1$, the point $v = (\alpha M \ \alpha(b+1))_{\mathrm{ref}} \in L^{\mathrm{np}}$ works.

The coordinates of these v are always in $[|0, N-1|]$, and coprime. By Remark 1, the reduction modulo N of the pair of the coordinates of v in the reference basis is a basis of a free, rank-1 sub-module of $(\mathbb{Z}/N\mathbb{Z})^2$. □

Proposition 5. *The induced map* $\mathrm{P}\mathcal{L}_1^N \to \mathbb{P}^1(\mathbb{Z}/N\mathbb{Z})$ *is injective.*

Proof. Consider two projective lattices $L, K \in \mathrm{P}\mathcal{L}_1^N$ mapped to the same class $[c:d] \in \mathbb{P}^1(\mathbb{Z}/N\mathbb{Z})$. The set of points in L^{np} with coordinates in $[|0, N-1|]$ coincide with the set of points of K^{np} with coordinates in $[|0, N-1|]$, hence $L^{\mathrm{np}} = K^{\mathrm{np}}$ (since they share the subgroup $N \cdot L_1^{np}$ and coincide on $L_1^{np}/(N \cdot L_1^{np})$), hence $K = L$. □

Example 1. *The projective lattice* L_2 *(see Appendix* A*) is* 2*-hyperdistant from* L_1*, and*

$$L_2^{\mathrm{np}} = \mathbb{Z} \cdot (2 \ 0) + \mathbb{Z} \cdot (0 \ 1)$$

Even if $2 \cdot (L_2^{\mathrm{np}})$ *is a sublattice of* L_1^{np} *of index* 8*, its projective class is still* L_2*. The reduction* $\mathrm{red}_8(2 \cdot (L_2^{\mathrm{np}}))$ *is the following submodule of* $(\mathbb{Z}/8\mathbb{Z})^2$*:*

$$\{(0,0), (0,2), (0,4), (0,6), (4,0), (4,2), (4,4), (4,6)\} \ .$$

which is obviously not free. Figure 1 *illustrates the relationship between* $\mathcal{L}_1^4$ *and the rank-*1 *free submodules of* $\mathbb{Z}/4\mathbb{Z}$*.*

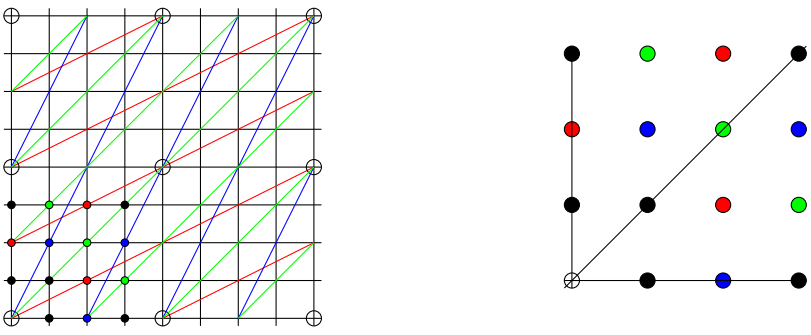


Figure 1: The underlying black lattice on the left is L_1^{np}, and three of its sublattices of index 4 are shown as the intersection points of L_1^{np} with, respectively, the red, blue and green lines. On the right, one sees in the $(\mathbb{Z}/4\mathbb{Z})^2$-plane, six of its free submodules of rank 1: the three lines in black, corresponding to the coordinates $[0:1]$, $[1:0]$ and $[1:1]$, as well as the red ([1:2]), green ([3:1]) and blue ([2:1]) lines which are the images of the corresponding sublattices on the left. Those six submodules are in fact all the free submodules of $(\mathbb{Z}/4\mathbb{Z})^2$ of rank 1 (see next section).

Proposition 6. *Let $c, d \in [|0, N-1|]$ be two coprime numbers. The free module corresponding to the class $[c:d] \in \mathbb{P}^1(\mathbb{Z}/N\mathbb{Z})$ defines a unique non-projective sublattice $L^{\mathrm{np}}_{[c:d]}$ of L_1^{np} of index N. Its projectivisation $L_{[c:d]}$ is in $\mathrm{P}\mathcal{L}_1^N$, and the image of $L_{[c:d]}$ under the map of Proposition 5 is $[c:d]$.*

Proof. Since $\gcd(c,d) = 1$, there exist $a, b \in \mathbb{Z}$ such that $ad - bc = 1$. Consider the map

$$[c:d] \to \text{Ł}^{\mathrm{np}}_{[c:d]} = \mathrm{SL}_2(\mathbb{Z}) \cdot \begin{pmatrix} Na & Nb \\ c & d \end{pmatrix}$$

The lattice $L^{\mathrm{np}}_{[c:d]}$ is obviously a sublattice of L_1^{np} of index N. Now since $ad - bc = 1$, the minimal $\alpha \in \mathbb{Q}^*_{>0}$ such that αa, αb, αc and αd are integers is 1, hence the projectivisation $L_{[c:d]}$ of $\text{Ł}^{\mathrm{np}}_{[c:d]}$ is N-hyperdistant from L_1. It is easy to see that the map above is the reciprocal of the one of Proposition 5. □

We have proved the following.

Theorem 1. *The set $\mathrm{P}\mathcal{L}_1^N$ is in bijection with the projective line $\mathbb{P}^1(\mathbb{Z}/N\mathbb{Z})$. Moreover, if $L \in \mathrm{P}\mathcal{L}_1^N$ corresponds to some $[c:d] \in \mathbb{P}^1(\mathbb{Z}/N\mathbb{Z})$ with $c, d \in [|0, N-1|]$ coprime numbers, the class of L in $\mathrm{PSL}_2(\mathbb{Z})\backslash\mathrm{PGL}_2^+(\mathbb{Q})$ is:*

$$\mathrm{PSL}_2(\mathbb{Z}) \cdot \begin{pmatrix} Na & Nb \\ c & d \end{pmatrix}$$

for some $a, b, c, d \in \mathbb{Z}$ such that $ad - bc = 1$.

Proposition 7. *Let L be a projective lattice N-hyperdistant from L_1. Then*

$$(L^{\mathrm{np}})/(N \cdot L_1^{\mathrm{np}}) \simeq (\mathbb{Z}/N\mathbb{Z}) \simeq L_1^{\mathrm{np}}/(L^{\mathrm{np}}) \ .$$

Proof. We have shown that there are $a, b \in [|0, N-1|]$ coprimes, such that $(a\ b) \in L^{\mathrm{np}}$. Let $c, d \in \mathbb{Z}$ such that $ad - bc = 1$.

1. Let $k \in \mathbb{Z}$ such that $k \cdot (a\ b) \in (N \cdot L_1^{\mathrm{np}})$. Then $N|ka$ and $N|kb$ hence $N|k(ad - bc)$ which proves

   $$(\text{Ł}^{\mathrm{np}})/(N \cdot L_1^{\mathrm{np}}) \simeq (\mathbb{Z}/N\mathbb{Z}) \ .$$

   Now let us take $p \in L$. Then $\mathrm{red}_N(p) = m \cdot (a\ b)$ for some $m \in \mathbb{Z}/N\mathbb{Z}$ hence $L = \mathbb{Z}(a\ b) + N \cdot L_1$.

2. Consider the vector $(c\ d) \in L_1^{\mathrm{np}}$, and $k \in \mathbb{Z}$ such that $k \cdot (c\ d) \in L^{\mathrm{np}}$, that is, $k(c\ d) = k'(a\ b) + (l_1 N, l_2 N)$ for $k', l_1, l_2 \in \mathbb{Z}$. Then $N|(kc - k'a)$ and $N|(kd - k'b)$ hence N divides $-b(kc - k'a) + a(kd - k'd) = k(ad - bc) = k$, and thus:

   $$(\mathbb{Z}/N\mathbb{Z}) \simeq L_1^{\mathrm{np}}/(\text{Ł}^{\mathrm{np}}) \ .$$

□

1.2 The bijection $\mathrm{P}\mathcal{L}_1^N \simeq \Gamma_0(N)\backslash\Gamma_0(1)$

Proposition 8. *Let $N \in \mathbb{N}_{>0}$. The right-action of $\Gamma_0(1)$ on $\mathrm{P}\mathcal{L}_1$ fixes the set $\mathrm{P}\mathcal{L}_1^N$. Moreover, the projective lattice $L_N \cdot M$ depends solely on the class of M in $\Gamma_0(N)\backslash\Gamma_0(1)$.*

Proof. The projective determinant is invariant under the right-action of $\mathrm{PSL}_2(\mathbb{Z}) = \Gamma_0(1)$, hence $\delta(L_N \cdot M, L_1 \cdot M) = \delta(L_N \cdot M, L_1) = \delta(L_N, L_1) = N$. Let $M, M' \in \Gamma_0(1)$ such that $L_N \cdot M' = L_N \cdot M$. Then

$$L_N \cdot M'M^{-1} = L_N \ ,$$

hence by definition of $\Gamma_0(N)$, $M'M^{-1} \in \Gamma_0(N)$, that is, $M' = AM$ with $A \in \Gamma_0(N)$. □

The cardinality of $\mathrm{P}\mathcal{L}_1^N$ is thus an upper-bound for the index of $\Gamma_0(N)$ in $\Gamma_0(1)$, hence Theorem 1 implies that $[\Gamma_0(1) : \Gamma_0(N)] < \infty$ for all $N \in \mathbb{N}_{>0}$. Let $\{\beta_i\}_{i\in I}$ be a set of representatives for the elements of $\Gamma_0(N)\backslash\Gamma_0(1)$ (one for each class). Then

$$\Gamma_0(1) = \bigcup_{i\in I} \Gamma_0(N) \cdot \beta_i$$

Remark 2. *Let $c, d \in [|0, N-1|]$ be two coprime numbers. Theorem 1 shows that:*

$$[c : d] \cdot M = [c : d] \cdot \begin{pmatrix} k & l \\ m & n \end{pmatrix} = \begin{pmatrix} Na & Nb \\ c & d \end{pmatrix} \begin{pmatrix} k & l \\ m & n \end{pmatrix} \tag{5}$$

$$[c : d] \cdot M = \begin{pmatrix} N(ak + bm) & N(al + bn) \\ ck + dm & cl + dn \end{pmatrix} = [ck + dm : cl + dn] \tag{6}$$

which yields a very explicit formula for the action of $\Gamma_0(1)$ on $\mathrm{P}\mathcal{L}_1^N$.

Proposition 9. *The right-action of $\Gamma_0(1)$ on $\mathrm{P}\mathcal{L}_1^N$ is transitive, and the bijection:*

$$\mathrm{P}\mathcal{L}_1^N \simeq \Gamma_0(N)\backslash\Gamma_0(1)$$

holds. Note that the projective lattice where $[0 : 1] \in \mathrm{P}\mathcal{L}_1^N$ corresponds to the class $\Gamma_0(N) \cdot 1$.

Proof. Since for all $c, d \in [|0, N-1|]$ such that $\gcd(c, d) = 1$, there exists $a, b \in \mathbb{Z}$ such that $ad - bc = 1$, and since $[c : d] = [0 : 1] \cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, the action is transitive. By definition, $\mathrm{Stab}_{\Gamma_0(1)}([0 : 1]) = \Gamma_0(N)$. □

1.3 Sets of representatives for $\mathbb{P}^1(\mathbb{Z}/N\mathbb{Z})$

Let us wrap-up what we have done, and show how to assign a single element in $[|0, N-1|]^2$ to a rank-1 free $\mathbb{Z}/N\mathbb{Z}$-submodule of $(\mathbb{Z}/N\mathbb{Z})^2$.

Let $a, b \in [|0, N-1|]$ such that $\gcd(a, b) = 1$. To the class $[a : b]$ corresponds a rank-1 free $\mathbb{Z}/N\mathbb{Z}$-submodule of $(\mathbb{Z}/N\mathbb{Z})^2$, but this map is many-to-one in general. The possible bases of this module are indeed the elements of the orbit:

$$(\mathbb{Z}/N\mathbb{Z})^\times \cdot (a, b) \ . \tag{7}$$

One may agree on some conventions to choose one representative for each class. One way to do it is as follows.

- Consider the set $\tilde{D}$ of orbits of the action of $(\mathbb{Z}/N\mathbb{Z})^\times$ on $\mathbb{Z}/N\mathbb{Z} \simeq [|0, N-1|]$. Let also D be the set containing the smallest element of each orbit.
- For each $d \in D$, consider the stabiliser $G = \mathrm{Stab}_{(\mathbb{Z}/N\mathbb{Z})^\times}\{d\}$. Let $\tilde{C_d}$ be the set of orbits of the action of G on the set of elements in $\mathbb{Z}/N\mathbb{Z}$ which are coprime with d. Let C_d be the set containing the smallest element of each orbit.

For all $a, b \in [|0, N-1|]$, there is a pair $(c, d) \in C_d \times D$ in the $(\mathbb{Z}/N\mathbb{Z})^\times$-orbit of (a, b).

Example 2. *Let $N = 6$, in which case:*

$$(\mathbb{Z}/6\mathbb{Z})^\times = \{1, 5\} \ .$$

Its orbits when acting on $\mathbb{Z}/6\mathbb{Z}$ are

$$\{\{0\}, \{1, 5\}, \{2, 4\}, \{3\}\} \ ,$$

thus $D = \{0, 1, 2, 3\}$, and

$$\begin{cases} \mathrm{Stab}_{(\mathbb{Z}/6\mathbb{Z})^\times}\{0\} = (\mathbb{Z}/6\mathbb{Z})^\times \\ \mathrm{Stab}_{(\mathbb{Z}/6\mathbb{Z})^\times}\{1\} = \{1\} \\ \mathrm{Stab}_{(\mathbb{Z}/6\mathbb{Z})^\times}\{2\} = \{1\} \\ \mathrm{Stab}_{(\mathbb{Z}/6\mathbb{Z})^\times}\{3\} = (\mathbb{Z}/6\mathbb{Z})^\times \end{cases} ,$$

hence

$$\begin{cases} C_0 = \{1\} \\ C_1 = \{0, 1, 2, 3, 4, 5\} \\ C_2 = \{1, 3, 5\} \\ C_3 = \{1, 2\} \end{cases} .$$

A set of representatives for $\mathbb{P}^1(\mathbb{Z}/6\mathbb{Z})$ is:

$$\{(1,0), (0,1), (1,1), (2,1), (3,1), (4,1), (5,1), (1,2), (3,2), (5,2), (1,3), (2,3)\} \subset (\mathbb{Z}/N\mathbb{Z})^2$$

From this we know that the set $\mathrm{P}\mathcal{L}_1^6$ is exactly:

$$\mathrm{P}\mathcal{L}_1^6 = \{L_{1/6}; L_6; L_{1/6,1/6}; L_{2/3,1/3}; L_{3/2,1/2}; L_{2/3,2/3}; L_{1/6,5/6};$$
$$L_{1/6,1/3}; L_{3/2}; L_{1/6,2/3}; L_{1/6,1/2}; L_{2/3}\} \ ,$$

where:

$$L_{1/6} = \mathrm{PSL}_2(\mathbb{Z}) \cdot \begin{pmatrix} 0 & -6 \\ 1 & 0 \end{pmatrix}, \qquad L_6 = \mathrm{PSL}_2(\mathbb{Z}) \cdot \begin{pmatrix} 6 & 0 \\ 0 & 1 \end{pmatrix},$$
$$L_{1/6,1/6} = \mathrm{PSL}_2(\mathbb{Z}) \cdot \begin{pmatrix} 0 & -6 \\ 1 & 1 \end{pmatrix}, \quad L_{2/3,1/3} = \mathrm{PSL}_2(\mathbb{Z}) \cdot \begin{pmatrix} 6 & 0 \\ 2 & 1 \end{pmatrix},$$
$$L_{3/2,1/2} = \mathrm{PSL}_2(\mathbb{Z}) \cdot \begin{pmatrix} 6 & 0 \\ 3 & 1 \end{pmatrix}, \qquad L_{2/3,2/3} = \mathrm{PSL}_2(\mathbb{Z}) \cdot \begin{pmatrix} 6 & 0 \\ 4 & 1 \end{pmatrix},$$
$$L_{1/6,5/6} = \mathrm{PSL}_2(\mathbb{Z}) \cdot \begin{pmatrix} 6 & 0 \\ 5 & 1 \end{pmatrix}, \qquad L_{1/6,1/3} = \mathrm{PSL}_2(\mathbb{Z}) \cdot \begin{pmatrix} 0 & -6 \\ 1 & 2 \end{pmatrix},$$
$$L_{3/2} = \mathrm{PSL}_2(\mathbb{Z}) \cdot \begin{pmatrix} -6 & -6 \\ 3 & 2 \end{pmatrix}, \qquad L_{1/6,2/3} = \mathrm{PSL}_2(\mathbb{Z}) \cdot \begin{pmatrix} -12 & -6 \\ 5 & 2 \end{pmatrix},$$
$$L_{1/6,1/2} = \mathrm{PSL}_2(\mathbb{Z}) \cdot \begin{pmatrix} 0 & -6 \\ 1 & 3 \end{pmatrix}, \quad L_{2/3} = \mathrm{PSL}_2(\mathbb{Z}) \cdot \begin{pmatrix} 6 & 6 \\ 2 & 3 \end{pmatrix}.$$

Of course the procedure we are following here is a pure convention, and one is free to choose any other representatives one likes more. The next proposition shows for instance a set of representatives for the elements of $\mathbb{P}^1(\mathbb{Z}/N\mathbb{Z})$ in the case $N = p^\alpha$ with p prime, which does not coincide with the one one would obtain with the recipe of above.

Proposition 10. *When $N = p^\alpha$ with p prime and $\alpha \in \mathbb{N}_{>0}$, a set of representatives in $[|0, p^\alpha - 1|]^2$ for $\mathbb{P}^1(\mathbb{Z}/p^\alpha\mathbb{Z})$ is given by*

$$\begin{cases} (a,1) & a = 0, 1, 2..., p^\alpha - 1 \ ; \\ (1,b) & b = pk, \ k \in [|0, p^{\alpha-1} - 1|] \ . \end{cases}$$

Hence $|\mathbb{P}^1(\mathbb{Z}/p^\alpha\mathbb{Z})| = (p+1)p^{\alpha-1}$.

Proof. Let $(x, y) \in (\mathbb{Z}/(p^\alpha)\mathbb{Z})^2$. If y is invertible, let $a = y^{-1}x$, and then $(x, y) \sim (a, 1)$. If not, then $y = pl$ for some $l \in \mathbb{N}$ but since $\gcd(x, y) = 1$, it implies that x is invertible, and thus that $(x, y) \sim (1, b)$ for $b = x^{-1}y$. These representatives are never equivalent, and we have $p^\alpha + p^{\alpha-1} = (p+1)p^{\alpha-1}$ of them. □

Remark 3. *The relationship with the set of representatives one would have got after using the recipe explained above, is as follows. The representatives of the form $(a, 1)$ for $a \in [|0, p^\alpha - 1|]$ are obtained in both procedures, while for $(1, b)$ with b not invertible, one can write $b = b'k^\beta$ with b' invertible. Then $[1 : b] = [(b')^{-1} : k^\beta]$, and $((b')^{-1}, k^\beta)$ is the representative of the class $[1 : b]$ that one would have got out of the first method. When $N = p^\alpha$, it turns out that the choice of representatives given in* 10 *is often convenient.*

1.4 The Index Formula

Proposition 11. *Let $M, N \in \mathbb{N}$ be coprime numbers. Then*

$$\begin{array}{ccc} \mathbb{P}^1(\mathbb{Z}/MN\mathbb{Z}) & \to & \mathbb{P}^1(\mathbb{Z}/M\mathbb{Z}) \times \mathbb{P}^1(\mathbb{Z}/N\mathbb{Z}) \\ (c, d) & \mapsto & ((c_1, d_1), (c_2, d_2)) \end{array}$$

is a bijection. The pair (c, d) is a representative of the point $[c : d]$, and the c_i or d_i are the reductions of c and d modulo M and N, respectively.

Proposition 11 is none other than the Chinese remainder theorem, and from Proposition 10 we know that:

$$|\mathbb{P}^1(\mathbb{Z}/(p^\alpha)\mathbb{Z})| = (p+1)p^{\alpha-1} \ ,$$

hence the following holds.

Proposition 12.

$$|\mathbb{P}^1(\mathbb{Z}/N\mathbb{Z})| = N\prod_{p|N}(1+\frac{1}{p}) \ .$$

Proof. Write $N = \prod_i p_i^{\alpha_i}$. We have

$$|\mathbb{P}^1(\mathbb{Z}/N\mathbb{Z})| = \prod_i |\mathbb{P}^1(\mathbb{Z}/(p_i^{\alpha_i})\mathbb{Z})| = \prod_i (p_i+1)p_i^{\alpha_i-1} = N\prod_{p|N}(1+\frac{1}{p})$$

□

2 Dessins d'enfants and analytical modular curves

The isomorphism $\mathrm{PSL}_2(\mathbb{Z}) \simeq (\mathbb{Z}/2\mathbb{Z}) \star (\mathbb{Z}/3\mathbb{Z})$ induces a structure of bipartite fat graph on each of the sets $\Gamma_0(N)\backslash\Gamma_0(1)$. These bipartite fat graphs are called *dessin d'enfants*, after Grothendieck's famous *Esquisse d'une Programme* [Gro13] (see [Sch11, Sch94]). This additional structure on $\Gamma_0(N)\backslash\Gamma_0(1)$ gives an efficient and purely group-theoretic definition of the cusps of the classical modular curves $X_0(N)$. The parametrisation of the $\Gamma_0(N)\backslash\Gamma_0(1)$ of the last section is of good use in order to understand and handle these dessins d'enfants.

2.1 Generalities

We begin with some rudiments and notation. For a more detailed introduction to dessins d'enfants, we refer to the book [JW16].

2.1.1 Fat graphs

Definition 3. *A* **fat graph** *(or ribbon graph) is a connected simple graph $\Gamma = (V, E)$ together with a cyclic orientation of E_v for every $v \in V$, where $E_v \subset E$ is the set of edges incident to v.*

Remark 4. *If $\Gamma = (V, E)$ is a fat graph then for $e \in E$ an edge and $v \in V$ one of the two ends of e, it makes sense to speak of "the edge directly after e with respect to v".*

An edge e of a graph $\Gamma = (V, E)$ is oriented if one of its two ends has been chosen to be its source, and the other one, its target.

Definition 4. *Let $\Gamma = (V, E)$ be a fat graph with V and E finite. A face of length k is a cycle of oriented edges $(\vec{e}_1, ..., \vec{e}_k)$ such that:*

- *for all $i \in \mathbb{Z}/k\mathbb{Z}$, the source of $\vec{e}_{i+1}$ is the target of $\vec{e}_i$,*
- *e_{i+1} is the edge directly after e_i with respect to the target of $\vec{e}_i$.*

The faces form a partition of the set of oriented edges.

2.1.2 Cusps and genus

A fat graph gives rise to topological surfaces as follows. Let $\Gamma = (V, E)$ be a connected fat graph with finitely many edges and vertices. For each face F of Γ, let us glue the boundary of a topological 2-cell to F, following the cyclic orientation of the latter. The resulting topological oriented surface $\tilde{S}_\Gamma$ is thus obtained as a cell complex whose 1-skeleton is Γ, and is compact and connected. Instead of gluing copies of a disk one can also glue copies of once-punctured disks $\mathbb{D}^2\backslash\{0\}$, and that yields another topological connected surface S_Γ which can be obtained from $\tilde{S}_\Gamma$ by removing one point in the interior of each of faces in $\tilde{S}_\Gamma$. These points are called **cusps**.

Definition 5. *The genus $g(\Gamma)$ of a connected fat graph Γ is the genus of the closed surface $\tilde{S}_\Gamma$. More intrinsically, $g(\Gamma)$ is half the rank of the first homology group of the chain complex*

$$0 \longrightarrow \mathbb{Z}^{\text{faces}} \xrightarrow{d} \mathbb{Z}^E \xrightarrow{\delta} \mathbb{Z}^V \longrightarrow 0$$

2.1.3 Bipartite fat graphs

Definition 6. *A bipartite graph is a graph (V, E) for which the set V is written as the disjoint union of a set V_W of white vertices and a set V_B of black vertices:*

$$V = V_W \amalg V_B \ ,$$

and such that each edge $e \in E$ has one "white" end and one "black" end. A bipartite fat graph is a bipartite graph endowed with a fat structure.

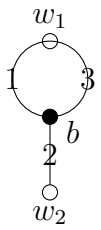


Figure 2: A bipartite graph drawn on a plane, whose counterclockwise orientation induces a fat structure on the graph. For example, the cyclic ordering of the edges around the black vertex is $1 < 2 < 3 < 1$. This fat graph has two faces, corresponding to the cycles $(1_{w_1\to b}, 2_{b\to w_2}, 2_{w_2\to b}, 3_{b\to w_1})$ (exterior face) and $(3_{w_1\to b}, 1_{b\to w_1})$ (inner face). Moreover $\tilde{S}_\Gamma \simeq \mathbb{S}^2$ and S_Γ has two cusps.

A bipartite fat structure on a graph $\Gamma = (V, E)$ singles out two permutations of its edges: a permutation $x \in \mathfrak{S}(E)$ which sends each edge to the next one with respect to its white end, and a permutation $y \in \mathfrak{S}(E)$ which sends each edge to the next one with respect to its black end.

Conversely, let x and y be two permutations of a set E, written as a product of disjoint circles. Let us define a bipartite fat graph $\Gamma = (V_W \amalg V_B, E)$ by setting V_W to be the set of cycles in x, V_B the set of cycles in y, and where an edge $e \in E$ links the only two vertices (one in V_W, one in V_B) that it "belongs" to. This construction is easily seen to be the inverse of the one of above.

This reasoning shows that any bipartite fat graph can be drawn on an oriented surface, in such a way that the fat structure at each vertex coincides with the counterclockwise orientation of the surface. We will follow this convention in the sequel. There might be crossings among the edges, whener the genus of the surface on which the graph is frawn is smaller that the genus of the graph. Note that the group generated by x and y acts transitively on E if and only if Γ is connected.

Remark 5. *The cycles of (xy) (in our notations, the permutation group $\mathfrak{S}(E)$ acts on the right of E, hence x acts first, and them y) are in one-to-one correspondence with the faces of Γ, as follows. Let e be an edge of Γ. The two possible orientations for e are denoted $e_{w\to b}$ and $e_{b\to w}$. Then a cycle $(e_1, ..., e_k)$ with $e_i \in E$ for $i \in [|1, k|]$ corresponds to the face $(e_{1,b\to w}, f_{1,w\to b}, e_{2,b\to w}, f_{2,w\to b}..., e_{k,b\to w}, f_{k,w\to b})$ of Γ, where each f_i labels the edge directly after e_i with respect to the white end of the latter.*

2.1.4 Algebraic Bipartite Maps and Dessins d'Enfants

Definition 7. *An algebraic bipartite map (ABM) is a quadruple*

$$\mathcal{B} = (G, x, y, E) \ ,$$

where E is a set, $x, y \in \mathfrak{S}(E)$, and such that $G = \langle x, y\rangle$ acts transitively on the right of E. The group G is called the **monodromy group** *(or* **cartographic group***) of $\mathcal{B}$. If E is a finite set, then $\mathcal{B}$ is called a* **dessin d'enfant** *(***dessin***, for short). The type of the ABM is the triple (a, b, c) where a (resp. b, c) is the order of x (resp. y, xy).*

Definition 8. *A morphism of ABMs $(G, x, y, E) \to (G', x', y', E')$ is a pair*

$$\left\{ \begin{array}{l} f : E \to E' \\ \phi : G \to G' \end{array} \right\} \ ,$$

where f is a morphism of sets, and ϕ a morphism of groups satisfying $\phi(x) = x'$ and $\phi(y) = y'$, and such that for all $e \in E$ and $g \in G$:

$$f(e) \cdot \phi(g) = f(e \cdot g) \ .$$

A morphism of dessins is a morphism of ABMs between two dessins.

For instance, the dessin d'enfant corresponding to the bipartite fat graph shown in Figure 2 is $(\mathfrak{S}_3, (13), (123), \{1, 2, 3\})$.

2.1.5 Automorphism group

Definition 9. *Let $\mathcal{B} = (G, x, y, E)$ be an ABM. The automorphism group $\mathrm{Aut}(\mathcal{B})$ of $\mathcal{B}$ is the centraliser of G in $\mathfrak{S}(E)$, that is, the group of permutations that commute with x and y. We will consider $\mathrm{Aut}(\mathcal{B})$ as acting on the left of E.*

Example 3. *Consider for example the dessin d'enfant of type $(2, 3, 2)$ in Figure 3. First,*

$$xy = (14)(26)(35)$$

and $G \simeq \mathfrak{S}_3 \simeq \mathrm{Aut}(\mathcal{B})$. *The automorphism group is generated by the rotation of order* 2 *around the central vertex, represented by the permutation* $(14)(36)(25)$, *and the rotation of order* 3 *around the black vertices, represented by* $(123)(654)$. *The topological surface* $S_{\mathcal{B}}$ *is a sphere with three cusps. Note here the difference between the monodromy group and the automorphism group. The latter is a group of symmetrie and is* **not** *generated (while the monodromy group is) by the local cyclic order around the vertices.*

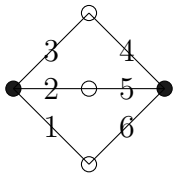


Figure 3: The dessin $\mathcal{B} = (G = \langle x, y\rangle, x = (16)(34)(25), y = (123)(456), [|1, 6|])$

The action of a group G on a set E is said to be

transitive if $\forall e, e' \in E$, there is at least one $g \in G$ such that $e' = e \cdot g$;

semi-regular if $\forall e, e' \in E$, there is at most one $g \in G$ such that $e' = e \cdot g$;

regular if $\forall e, e' \in E$, there is exactly one $g \in G$ such that $e' = e \cdot g$.

The following two results on automorphisms of ABMs correspond respectively to Theorem 2.1 and Corollary 2.1 in [JW16], where the proof of these statements can be found.

Proposition 13. *Let* $\mathcal{B} = (G, x, y, E)$ *be an ABM. Then*

1. $\mathrm{Aut}(\mathcal{B})$ *acts semi-regularly on* E;
2. $\mathrm{Aut}(\mathcal{B})$ *acts regularly on* E *if and only if* G *does, and in that case* $G \simeq \mathrm{Aut}(\mathcal{B})$.

In the latter case one says that the ABM is **regular**.

Proposition 14. *Let* (G, x, y, E) *be an ABM, and* $e \in E$. *Let* $G_e = \mathrm{Stab}_G(e)$. *Then*

$$\mathrm{Aut}(\mathcal{B}) \simeq N_G(G_e)/G_e \ ,$$

where $N_G(G_e)$ *is the normaliser of* G_e *in* G.

2.1.6 Quotient of ABMs

Let $\mathcal{B} = (G, x, y, E)$ be an ABM, and let $H < \mathrm{Aut}(\mathcal{B})$. The left-quotient of $\mathcal{B}$ by H is another ABM denoted $H\backslash\mathcal{B}$ together with a morphism

$$\mathcal{B} \to H\backslash\mathcal{B}$$

The quotient $H\backslash\mathcal{B} = (G', x', y', E')$ is constructed as follows.

1. E' is the set of equivalence classes $H\backslash E$.
2. The permutation x' of E' is the one satisfying $[e] \cdot x' = [e \cdot x]$ for all $e \in E$.
3. Similarly, y' is the permutation of E' such that $[e] \cdot y' = [e \cdot y]$ for all $e \in E$.
4. One sets $G' = \langle x', y'\rangle$.

Remark 6. *If $\mathcal{B}$ is of type (p,q,r) then $H\backslash\mathcal{B}$ is of type (p',q',r') where $p'|p,\ q'|q,\ r'|r$.*

Example 4. *Consider the dessin d'enfant given in Figure 3:*

$$\mathcal{B} = (G = \langle x, y\rangle, x = (16)(34)(25), y = (123)(456), [|1,6|])$$

Let $H = \langle(16)(35)(24)\rangle < \mathrm{Aut}(\mathcal{B})$. The quotient $\mathcal{B} \to H\backslash\mathcal{B}$ is given schematically in Figure 4, and

$$H\backslash\mathcal{B} = (\mathfrak{S}_3, (13), (123), [|1,3|]) \ .$$

Figure 4: An example of a quotient of dessin d'enfants

2.1.7 $\Gamma_0(1)$ and the universal ABM of type $(2,3,\infty)$

Recall the standard presentation of $\mathrm{PSL}_2(\mathbb{Z}) = \Gamma_0(1)$

$$\Gamma_0(1) \simeq \mathrm{PSL}_2(\mathbb{Z}) \simeq C_2 \star C_3 = \langle S, U | S^2 = U^3 = 1\rangle \ . \tag{8}$$

Definition 10. *The universal ABM of type $(2,3,\infty)$ is the ABM*

$$\mathcal{B}_\infty = (\mathrm{PSL}_2(\mathbb{Z}), S, U, \mathrm{PSL}_2(\mathbb{Z}))$$

$$S := \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}, \ U := \begin{bmatrix} 0 & -1 \\ 1 & -1 \end{bmatrix}$$

where the action of the group $\mathrm{PSL}_2(\mathbb{Z})$ on the set $\mathrm{PSL}_2(\mathbb{Z})$ corresponds to the group right-multiplication. This ABM is regular, all its white vertices are two-valent and all its black vertices are three-valent. It is universal in the sense that any ABM of type $(2,3,c)$ for some $c \in \mathbb{N}_{>0}$ is isomorphic to a quotient $H\backslash\mathcal{B}_\infty$ for some $H < \mathrm{Aut}(\mathcal{B}_\infty) = \mathrm{PSL}_2(\mathbb{Z})$.

Part of the corresponding bipartite fat graph is shown in Figure 5. It is easily obtained from the universal trivalent tree by the replacement of each vertex of the tree by a black vertex, and the addition of a white vertex in the middle of each edge.

2.1.8 Projective bases of L_1

The set of all oriented projective bases that generate L_1 can be identified with the set of edges of $\mathcal{B}_\infty$ via the map

$$\begin{bmatrix} f^1 \\ f^2 \end{bmatrix} \to \begin{bmatrix} f^1_1 & f^1_2 \\ f^2_1 & f^2_2 \end{bmatrix}$$

where the f^i_j are the coordinates of the vector f^i in the reference basis.

Since $\mathrm{PSL}_2(\mathbb{Z}) \simeq \langle S\rangle \star \langle U\rangle$, the set of edges of $\mathcal{B}_\infty$ corresponds to the words e, eS, and $e \cdot S^k U^{l_1} S U^{l_2} ... S^{k_n} U^{l_n} S^{k'}$ for integers $n \geq 0$, $k, k' \in [|0,1|]$ and $l_1, ..., l_n \in [|1,2|]$. Here e is a conventional "origin" associated with the identity matrix in $\mathrm{PSL}_2(\mathbb{Z})$.

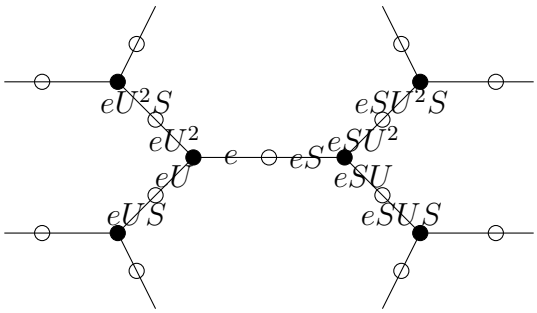


Figure 5: A part of $\mathcal{B}_\infty$, with reference edge e.

The map above associates $\mathrm{Id} \in \mathrm{PSL}_2(\mathbb{Z})$ to the reference projective basis in $\mathbb{P}V$. Any other projective basis that generate $L_1 \in \mathrm{PSL}_2(\mathbb{Z})\backslash\mathrm{PGL}_2^+(\mathbb{Q})$ is thus identified with the corresponding word of S's and U's. Note that

$$\begin{bmatrix} f_1^1 & f_2^1 \\ f_1^2 & f_2^2 \end{bmatrix} \cdot S = \begin{bmatrix} f_2^1 & -f_1^1 \\ f_2^2 & -f_1^2 \end{bmatrix}$$

and

$$\begin{bmatrix} f_1^1 & f_2^1 \\ f_1^2 & f_2^2 \end{bmatrix} \cdot U = \begin{bmatrix} f_2^1 & -(f_1^1 + f_2^1) \\ f_2^2 & -(f_1^2 + f_2^2) \end{bmatrix}$$

This right-action of $\mathrm{PSL}_2(\mathbb{Z})$ on $\mathrm{PSL}_2(\mathbb{Z})\backslash\mathrm{PGL}_2^+(\mathbb{Q})$ describes global projective linear transformations of V that preserve L_1.

However, if one considers a projective lattice N-hyperdistant from L_1, it is a priori not preserved by such a projective linear transformation in $\mathrm{PSL}_2(\mathbb{Z})$, but instead is mapped to another projective lattice N-hyperdistant from L_1 (since the right action of $\mathrm{PSL}_2(\mathbb{Z})$ preserves the hyperdistance). The dessins d'enfants which correspond to the Hecke groups $\Gamma_0(N)$ contains this data quite efficiently.

2.2 Definition of the dessins $\mathcal{B}_{0,N}$

Let $N \in \mathbb{N}_{>0}$. Since $\Gamma_0(N) < \mathrm{PSL}_2(\mathbb{Z}) = \mathrm{Aut}(\mathcal{B}_\infty)$, there is a quotient dessin:

$$\mathcal{B}_{0,N} = \Gamma_0(N)\backslash\mathcal{B}_\infty = (G_{0,N}, x_{0,N}, y_{0,N}, E_{0,N} = \Gamma_0(N)\backslash\Gamma_0(1)) \ . \tag{9}$$

We will soon see that if $N \geq 2$ those dessins are of type (a, b, c) with:

$$a = 2, \ b = 3, \ c = N \ . \tag{10}$$

Of course the case $N = 1$ corresponds to the trivial dessin with E a singleton.

Let $X_0(N) = \tilde{S}_{\mathcal{B}_{0,N}}$ (resp. $Y_0(N) = S_{\mathcal{B}_{0,N}}$) be the closed topological surface (resp. the topological surface with cusps) associated with $\mathcal{B}_{0,N}$. The groups $\Gamma_0(N)$ inherit a genus and a set of cusps from their corresponding dessin.

2.2.1 Canonical morphisms

Let $N, d \in \mathbb{N}_{>0}$ with d dividing N. Since $\Gamma_0(N) \leq \Gamma_0(d) \leq \Gamma_0(1)$ one has the following.

Proposition 15. *There is a canonically defined morphism*

$$(f, \phi)_{N,d} : \mathcal{B}_{0,N} \to \mathcal{B}_{0,d}.$$

Proof. Since $\Gamma_0(N) \leq \Gamma_0(d)$ are subgroups of finite index in $\Gamma_0(1)$, the group $\Gamma_0(N)$ has also finite index in $\Gamma_0(d)$. Let $I_{N,d} = [\Gamma_0(d) : \Gamma_0(N)]$. One has:

$$\Gamma_0(1) = \coprod_{j=1}^{I_{d,1}} \Gamma_0(N) \cdot \beta_j \ ,$$

$$\Gamma_0(d) = \coprod_{i=1}^{I_{N,d}} \Gamma_0(N) \cdot \alpha_i \ .$$

This yields

$$\Gamma_0(1) = \coprod_{i,j} \Gamma_0(N) \cdot (\alpha_i \beta_j) \ ,$$

hence

$$\Gamma_0(N) \backslash \Gamma_0(1) \simeq \Gamma_0(d) \backslash \Gamma_0(1) \times \Gamma_0(N) \backslash \Gamma_0(d) \ .$$

Let f be the projection $\Gamma_0(N)\backslash\Gamma_0(1) \to \Gamma_0(d)\backslash\Gamma_0(1)$, and

$$\phi : \langle x_{0,N}, y_{0,N} \rangle \leq \mathfrak{S}(E_{0,N}) \to \langle x_{0,d}, y_{0,d} \rangle \leq \mathfrak{S}(E_{0,d})$$

the group morphism with domain the group generated by $(x_{0,N}, y_{0,N})$ and target the group generated by $(x_{0,d}, y_{0,d})$. It is defined by $\phi(x_{0,N}) = x_{0,d}$ and $\phi(y_{0,N}) = y_{0,d}$.

Let $e \in \mathrm{PSL}_2(\mathbb{Z}) = E(\mathcal{B}_\infty)$. By definition of the quotient, $(\Gamma_0(N) \cdot e) \cdot x_{0,N} = \Gamma_0(N) \cdot (e \cdot x)$, and $(\Gamma_0(d) \cdot e) \cdot x_{0,d} = \Gamma_0(d) \cdot (e \cdot x)$ where $x = x_{0,1}$. Subsequently:

$$f((\Gamma_0(N) \cdot e) \cdot x_{0,N}) = f(\Gamma_0(N) \cdot (e \cdot x)) = \Gamma_0(d) \cdot (e \cdot x) = (\Gamma_0(d) \cdot e) \cdot x_{0,d} \ .$$

The same reasoning holds for the y's hence

$$(f, \phi) : \mathcal{B}_{0,N} \to \mathcal{B}_{0,d}$$

is a morphism of dessin d'enfants. □

Example 5. *The morphism* $(f, \phi)_{6,2} : \mathcal{B}_{0,6} \to \mathcal{B}_{0,2}$ *satisfies* $f_{6,2}^{-1}(\{1\}) = \{1, 7, 6, 12\}$, $f_{6,2}^{-1}(\{2\}) = \{2, 4, 8, 10\}$ *and* $f_{6,2}^{-1}(\{3\}) = \{3, 5, 9, 11\}$. *It is pictured in Figure* 6.

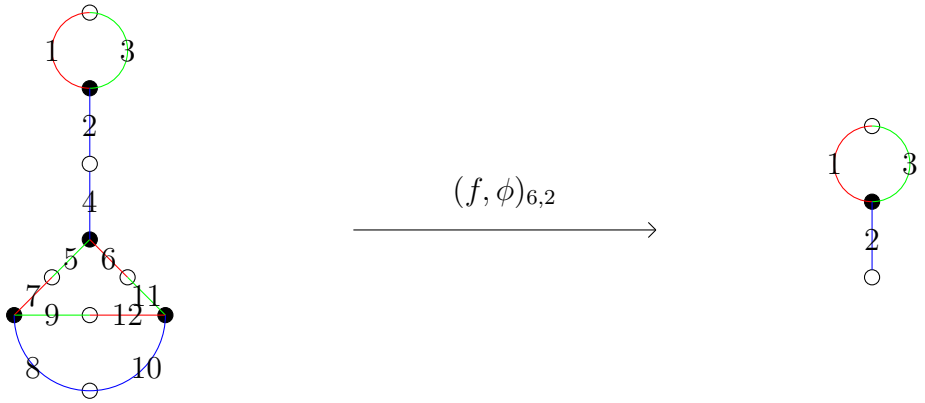


Figure 6: The canonical morphism $(f, \phi)_{6,2} : \mathcal{B}_{0,6} \to \mathcal{B}_{0,2}$, illustrating Proposition 15.

2.2.2 Naming the edges

Theorem 1 implies that one can choose representatives of the elements of $\Gamma_0(N)\backslash\Gamma_0(1)$ as a set of pairs of coprime numbers in $[|0, N-1|]$.

When $N = p^\alpha$ with p a prime number and $\alpha \in \mathbb{N}_{>0}$, we have seen that

$$\{(a,1),(1,b)|\ a \in \mathbb{Z}/p^\alpha\mathbb{Z},\ b \in p\mathbb{Z}/p^\alpha\mathbb{Z}\}$$

conveniently represents the points of $\mathbb{P}^1(\mathbb{Z}/p^\alpha\mathbb{Z})$.

As already emphasized, there is in general no natural choice of representatives. However, it is easy to construct such a set of representatives, since Remark 2 implies that:

$$[c:d] \cdot x_{0,N} = [d:-c]$$

$$[c:d] \cdot y_{0,N} = [d:-(c+d)]$$

Hence one can built $\mathcal{B}_{0,N}$ edge by edge, in a very hands-on way.

Example 6. *Let us draw $\mathcal{B}_{0,11}$. We could use the special set of representatives listed above since 11 is prime, however, we will construct the dessin directly to illustrate the general case. Let us start with the projective lattice L_{11} (which corresponds to $[0:1]$), and compute:*

$$\begin{array}{ccc}
[0:1]x_{0,11} = [1:0] & [0:1]y_{0,11} = [1:-1] = [10:1] & [0:1]y_{0,11}^2 = [1:0] \\
[10:1]x_{0,11} = [1:1] & [1:1]y_{0,11} = [1:-2] = [5:1] & [1:1]y_{0,11}^2 = [1:-6] = [9:1] \\
[5:1]x_{0,11} = [2:1] & [2:1]y_{0,11} = [7:1] & [2:1]y_{0,11}^2 = [4:1] \\
[9:1]x_{0,11} = [6:1] & [6:1]y_{0,11} = [3:1] & [6:1]y_{0,11}^2 = [8:1]
\end{array}$$

This is enough to completely determine $\mathcal{B}_{0,11}$: it has two faces, corresponding to the cycles $([1:0])$ and $([a:1])_{a\in[|0,10|]}$, and its genus is 1. The corresponding bipartite fat graph is given in Figure 7.

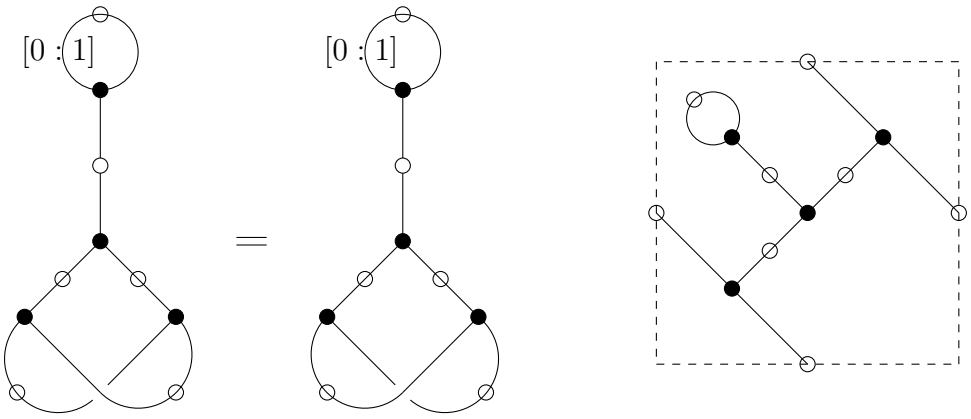


Figure 7: The bipartite fat graph corresponding to $\mathcal{B}_{0,11}$.

2.2.3 Interpretation of the Hecke dessins in terms of lattices

We know that the set of edges of the universal bipartite map $\mathcal{B}_\infty$ of type $(2,3,\infty)$ is the set of projective bases for the projective lattice L_1. Choose a projective lattice N-hyperdistant from L_1, say, L_N. It corresponds to the following coset in $\mathrm{PSL}_2(\mathbb{Z})\backslash\mathrm{PGL}_2^+(\mathbb{Q})$:

$$\mathrm{PSL}_2(\mathbb{Z}) \cdot \begin{pmatrix} N & 0 \\ 0 & 1 \end{pmatrix} .$$

Under a projective linear transformation of the vector space V preserving L_1 (i.e., under the right multiplication by a matrix in $\mathrm{PSL}_2(\mathbb{Z})$), L_N is mapped to a projective lattice N-hyperdistant from L_1, which is a priori different from L_N.

Since any matrix in $\mathrm{PSL}_2(\mathbb{Z})$ can be written as a product of S's and U's, the dessin d'enfant corresponding to $\Gamma_0(N)$ describes how these "elementary" projective transformations act on the set $\mathcal{L}_1^N$:

- there is a bijection between the set of edges in $\mathcal{B}_{0,N}$ and the set $\mathcal{L}_1^N$,
- if one right-multiplies the class corresponding to a projective lattice by S (resp. U), one obtains the class corresponding to the projective lattice associated with the edge directly after the one we started with, with respect to the white (resp. black) end of the latter.

In the next subsection we study the cusps of the $\mathcal{B}_{0,N}$, i.e the cycles of the permutation $y_{0,N}x_{0,N}$. In terms of projective lattices, a cusp is a cycle for the projective transformation US acting on $\mathcal{L}_1^N$.

2.3 Torsion points, cusps and genus of the $\mathcal{B}_{0,N}$

2.3.1 Torsion points of order 2

Definition 11. *The torsion points of order* 2 *in* $\mathcal{B}_{0,N}$ *are the one-valent white vertices of* $\mathcal{B}_{0,N}$.

Let $c, d \in [|0, N-1|]$ be coprimes, and such that $[c:d]$ corresponds to the edge terminating at such a torsion point of order 2. Since the latter is one-valent, we know that:

$$[c:d] \cdot x_{0,N} = [d:-c] = [c:d] ,$$

hence there exists $k \in [|0, N-1|]$ satisfying $\gcd(k, N) = 1$, and such that $c = kd$ and $d = -kc$ in $\mathbb{Z}/N\mathbb{Z}$. This implies $-(c,d) = k^2(c,d)$, and $k^2 = -1$ (using Bezout's identity). Therefore, if -1 is not a quadratic residue modulo N, there cannot be any white vertex of valency one in $\mathcal{B}_{0,N}$. One can refine this analysis into an actual counting of the number of torsion points of order 2 in $\mathcal{B}_{0,N}$, as follows.

The case $N = p^\alpha$ with $p > 2$ Consider the case $N = p^\alpha$ where $p > 2$ is a prime number, and $\alpha \in \mathbb{N}_{>0}$. In that case, the representatives $(c,d) \in [|0, N-1|]^2$ of the points of $\mathbb{P}^1(\mathbb{Z}/N\mathbb{Z})$ have at least one coordinate which is coprime with p^α, since $\gcd(c, d, p^\alpha) = 1$, hence the representative of any edge can be chosen of the form $(c, 1)$, with $c \in \mathbb{Z}/p^\alpha\mathbb{Z}$, as already explained above.

Let us assume that the white end of the edge $[c:1]$ is of one-valent. Right-multiplication by x_{0,p^α} yields $[1:-c]$, which has to be the same point as $[c:1]$, because of the assumption on the valency of the white end. Hence $c^2 = -1$ in $\mathbb{Z}/p^\alpha\mathbb{Z}$, which implies that the order of $c$in the group $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ is 4.

It is a classical result that:

$$(\mathbb{Z}/p^\alpha\mathbb{Z})^\times \simeq (\mathbb{Z}/(p-1)p^{\alpha-1}\mathbb{Z}) \ ,$$

though not canonically. Anyways, since this group is cyclic, the equation $x^2 = -1$ has exactly two solutions if and only if $4|(p-1)p^{\alpha-1}$, that is, if and only if $p \equiv 1[4]$.

The case $N = 2^\alpha$ Now consider the case $p = 2$, and $\alpha \in \mathbb{N}_{>0}$.

- If $\alpha = 1$, the group $(\mathbb{Z}/2\mathbb{Z})^\times$ is trivial. Hence the equation $x^2 = -1 = 1$ has $x = 1$ as unique solution.
- Assume nom that $\alpha > 1$. The invertibles in $\mathbb{Z}/2^\alpha\mathbb{Z} \simeq [|0, 2^\alpha - 1|]$ are the odd numbers. A square root of -1 hence corresponds to a solution of the equation

  $$(2y+1)^2 = l2^\alpha - 1 \ ,$$

  for some $y, l \in \mathbb{Z}$. This is equivalent to $4k^2 + 4k + 1 = l2^\alpha - 1$, and hence to $2k^2 + 2k = l2^{\alpha-1} - 1$. This equation has no solution in $\mathbb{Z}$ since we assumed that $\alpha > 1$.

General N Let $N \in \mathbb{N}_{>0}$, and decompose N in prime factors: $N = \prod_i p_i^{\alpha_i}$. The Chinese remainder theorem states that

$$\mathbb{Z}/N\mathbb{Z} \simeq \prod_i \mathbb{Z}/p_i^{\alpha_i}\mathbb{Z} \ ,$$

hence $x \in (\mathbb{Z}/N\mathbb{Z})$ satisfies $x^2 = -1$ if and only if $(\mathrm{red}_{p_i^{\alpha_i}}(x))^2 = -1$ in $\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z}$ for all i. Conversely, remember that for coprimes M and N, one has $E_{0,MN} = E_{0,M} \times E_{0,N}$, hence any tuple (x_i) such that for all i, $x_i^2 \equiv -1$ mod. $p_i^{\alpha_i}$, corresponds to a solution of the equation $x^2 = -1$ in $(\mathbb{Z}/N\mathbb{Z})$. We have then proved the following:

Proposition 16. *Let $N \in \mathbb{N}_{>0}$, and decompose it in prime factors:*

$$N = 2^a \times \prod_{i=1}^{n} p_i^{\alpha_i}, \ \forall i \in [|1,n|], \ \alpha_i > 0 \ .$$

Then $\mathcal{B}_{0,N}$ has torsion points of order 2 if and only if $a \leq 1$ and for all $i \in [|1,n|]$, $p_i \equiv 1$ modulo 4, and $\alpha_i = 1$. In that case there are exactly 2^n different solutions to the equation $x^2 = -1$ in $(\mathbb{Z}/N\mathbb{Z})$, or equivalently, $\mathcal{B}_{0,N}$ has exactly 2^n torsion points of order 2.

2.3.2 Torsion points of order 3

Definition 12. *The torsion points of order 3 in $\mathcal{B}_{0,N}$ are the one-valent black vertices of $\mathcal{B}_{0,N}$.*

Let $c, d \in [|0, N-1|]$ coprimes such that $[c : d]$ is the edge terminating at such a torsion point of order 3. Since the latter is a one-valent vertex, we know that:

$$[c : d] \cdot y_{0,N} = [d : -(c+d)] = [c : d]$$

hence there exists $k \in [|0, N-1|]$ satisfying $\gcd(k, N) = 1$, and such that $c = kd$ and $d = -k(c+d)$ in $(\mathbb{Z}/N\mathbb{Z})$. This implies that $(k^2+k+1)c = 0$, together with $(k^2+k+1)d = 0$, and again thanks to Bezout's identity: $k^2+k+1 = 0$. Multiplying both sides of $k^2+k+1 = 0$ by k yields $k^3 = 1$, but in general, $k^3 = 1$ does not imply $k^2+k+1 = 0$ in $\mathbb{Z}/N\mathbb{Z}$. However, we're going to be looking at the third roots of 1, and among them, which ones are solutions of $k^2+k+1 = 0$.

Let $N \in \mathbb{N}_{>0}$ be a power of a prime: $N = p^\alpha$. There cannot be any solution of the equation $k^2+k+1 = 0$ in $\mathbb{Z}/p^\alpha\mathbb{Z}$ if this ring does not admit any third roots of 1, and because we know the cyclic structure of the group of invertibles in $\mathbb{Z}/p^\alpha\mathbb{Z}$, we can conclude that the prime p has to be either 3 or congruent to 1 modulo 3. Let k be such that $k^3 = 1$, and set $a = k^2+k+1 \in \mathbb{Z}/p^\alpha\mathbb{Z}$. Multiplying both sides with k yields $ka = k^3 + (a-1) = a$, hence $(k-1)a = 0$.

The case $N = p^\alpha$ for $p > 3$ Let $p > 3$ be a prime, and let $N = p^\alpha$, with $\alpha \geq 1$. Since $N > 3$, $k = 1$ is not a solution of $k^2+k+1 = 0$, hence one must consider the other third roots of 1, if any. Suppose that $p \equiv 1$ mod. 3. Then, from the structure of the group $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$, we know that there are two third roots of 1 which are not 1. Let k be such a root. Then:

- Either $(k-1)$ is invertible, in which case $a = k^2+k+1$ has to be zero, since $(k-1)a = 0$.
- Otherwise, $(k-1)$ is not invertible, i.e. $k = pk+1$. Then $a = k^2+k+1 = p^2k^2+3pk+3$. We assumed that $p > 3$, thus a is invertible, and subsequently $k = 1$, which contradicts our initial hypothesis.

Hence the non-trivial third roots of 1 satisfy $k^2+k+1 = 0$.

The case $N = 3^\alpha$ For $\alpha = 1$ the trivial case $k = 1$ is the only solution of $k^2+k+1 = 0$, and we assume now that $\alpha > 1$.

One can check that $k_1 = (1+3^{\alpha-1})$ and $k_2 = (1-3^{\alpha-1})$ are the two non-trivial third roots of 1, and that $k_1^2+k_1+1 = k_2^2+k_2+1 = 3$. Hence if $\alpha > 1$ the equation $k^2+k+1 = 0$ has no solution on $\mathbb{Z}/3^\alpha\mathbb{Z}$.

General N Eventually, consider any $N \in \mathbb{N}_{>0}$, and decompose N in prime factors: $N = \prod_i p_i^{\alpha_i}$. The Chinese remainder theorem states that

$$\mathbb{Z}/N\mathbb{Z} \simeq \prod_i \mathbb{Z}/p_i^{\alpha_i}\mathbb{Z} \ ,$$

hence $x \in \mathbb{Z}/N\mathbb{Z}$ satisfies $x^2+x+1 = 0$ if and only if $\mathrm{red}_{p_i^{\alpha_i}}(x)$ satisfies this equation in $\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z}$ for all i. Conversely, remember that for coprimes M and N, one has $E_{0,MN} = E_{0,M} \times E_{0,N}$ hence any tuple (x_i) such that for all i, $x_i^2+x_i+1 = 0$ mod. $p_i^{\alpha_i}$, corresponds to a solution in $(\mathbb{Z}/N\mathbb{Z})$. Hence one has the following

Proposition 17. *Let $N \in \mathbb{N}_{>0}$, and decompose it in prime factors*

$$N = 3^a \times \prod_{i=1}^{n} p_i^{\alpha_i},\ \forall i \in [|1,n|],\ \alpha_i > 0\ .$$

Then $\mathcal{B}_{0,N}$ has torsion points of order 3 if and only if $a \leq 1$ and for all $i \in [|1,n|]$, $p_i \equiv 1$ modulo 3. In that case there are exactly 2^n different solutions in $\mathbb{Z}/N\mathbb{Z}$ to the equation $x^2 + x + 1 = 0$, and equivalently, $\mathcal{B}_{0,N}$ has exactly 2^n torsion points of order 3.

2.3.3 Description of the cusps and their width

Recall that the cusps of $\mathcal{B}_{0,N}$ are the cycles of the permutation $y_{0,N}x_{0,N}$. Let $\mathcal{C}(N)$ be the set of cusps in $\mathcal{B}_{0,N}$.

Note that $y_{0,1}x_{0,1} = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$, which implies $[c:d] \cdot (y_{0,N}x_{0,N}) = [c+d:d]$. The case $N = 8$ is partly studied as an example in Example 7 below.

Example 7. *Let $N = 8$, and choose the set of representatives $\{(c,1),\ c \in \mathbb{Z}/8\mathbb{Z}\} \cup \{(1,c),\ c \in 2\mathbb{Z}/8\mathbb{Z}\}$ for the homogeneous coordinates on $\mathbb{P}^1(\mathbb{Z}/8\mathbb{Z})$. Consider the projective lattice 8-hyperdistant from L_1 corresponding to the homogeneous coordinate $[1:6]$. The right-action of US yields the projective lattice corresponding to*

$$[6+1:6] = [-1:6] = [1:-6] = [1:2]\ ,$$

and $[1:2] \cdot US = [1:6]$. Hence the "central" cusp in $\Gamma_0(8)$ is the cycle of projective lattices corresponding to $([1:6],[1:2])$. One can compute that they are the projective lattices $(L_{1/8,3/4}, L_{1/8,1/4})$.

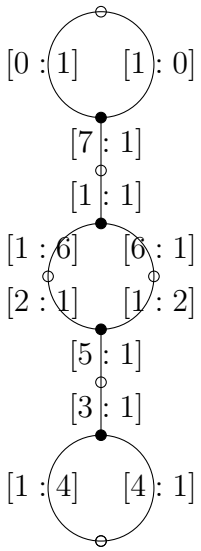


Figure 8: The dessin d'enfant $\mathcal{B}_{0,8}$.

Definition 13. *The width function*

$$w : \mathcal{C}(N) \to \mathbb{N}$$

associates to each cusp $c \in \mathcal{C}(N)$ the length of the corresponding cycle in the decomposition of $y_{0,N}x_{0,N}$ in disjoint cycles.

Proposition 18.

$$\sum_{c\in\mathcal{C}(N)} w(c) = |\mathbb{P}^1(\mathbb{Z}/N\mathbb{Z})| = N\prod_{p|N}(1+\frac{1}{p}) \ ,$$

where the last product runs over the prime numbers dividing N.

Proof. The sum of the length of all the cycles in the decomposition of the permutation $y_{0,N}x_{0,N}$ is the cardinality of $E_{0,N}$ which has already been shown to be $|\mathbb{P}^1(\mathbb{Z}/N\mathbb{Z})|$. □

Definition 14. *Let $N > 1$ be an integer. Then $\mathcal{B}_{0,N}$ has two special cusps denoted c_∞ and c_0, with width $w(c_\infty) = 1$ and $w(c_0) = N$.*

Proof. The cusp c_∞ is the singleton $\{[1:0]\}$, which is a cusp of width 1 since

$$[1:0]\cdot\begin{bmatrix}1&0\\1&1\end{bmatrix} = [1:0] \ .$$

Let now c_0 be the cusp defined as the one containing the edge $[0:1]$. Since

$$[0:1]\cdot\begin{bmatrix}1&0\\1&1\end{bmatrix}^k = [k:1] \ ,$$

and since $[N:1] = [0:1]$, the cusp c_0 is the cycle $([0:1],[1:1],...,[N-1:1])$ and has width N. □

Proposition 18 and definition 14 imply

Corollary 1. *Let $N = p$ a prime number. Then $\mathcal{C}(p) = \{c_0, c_\infty\}$.*

Proposition 19. *Let $N = p^\alpha$ with p prime. Then:*

$$|\mathcal{C}(p^\alpha)| = \sum_{0\le k\le\alpha}\phi(\gcd(p^k, p^{\alpha-k}))$$

where ϕ is Euler's totient function. Moreover, there is an explicit description of $\mathcal{C}(p^\alpha)$.

Proof. The points of $\mathbb{P}^1(\mathbb{Z}/p^\alpha\mathbb{Z})$ which are neither $[1:0]$ or of the form $[a:1]$ with $a\in\mathbb{Z}/p^\alpha\mathbb{Z}$ can be written $[1:p^k\beta]$ with $\gcd(\beta,p)=1$ and $0<k<\alpha$. Then:

$$[1:p^k\beta]\cdot\begin{bmatrix}1&0\\w&1\end{bmatrix} = [1+wp^k\beta : p^k\beta] = [1:\frac{p^k\beta}{1+wp^k\beta}] \ .$$

The smallest w such that

$$\frac{p^k\beta}{1+wp^k\beta} = p^k\beta \ (\Leftrightarrow wp^{2k}\beta^2 = 0) \tag{11}$$

holds in $\mathbb{Z}/p^\alpha\mathbb{Z}$, is the width of the cusp containing the projective lattice $[1:p^k\beta]$.

Now, since β and p are coprimes:

- either $2k\le\alpha$, and then the smallest w for which eq. 11 holds is $p^{\alpha-2k}$,
- or $2k>\alpha$ then the smallest w for which eq. 11 holds is 1.

In any case, $0\le\beta\le p^{\alpha-k}$, and since β and p are coprimes, there are $\phi(p^{\alpha-k})$ different possible β's, hence:

- either $2k \leq \alpha$, then there are

$$\frac{\phi(p^{\alpha-k})}{p^{\alpha-2k}} = \frac{p^{\alpha-k-1(p-1)}}{p^{\alpha-2k}} = p^{k-1}(p+1) = \phi(\gcd(p^k, p^{\alpha-k}))$$

  cusps containing points of the form $[1 : p^k\beta]$, all of width $p^{\alpha-2k}$,

- or $2k > \alpha$, and then there are $\phi(p^{\alpha-k}) = \phi(\gcd(p^k, p^{\alpha-k}))$ cusps of width 1.

Eventually, the points of the form $[a : 1]$ correspond to the special case $k = 0$. They form a unique cusp c_0 of width p^α. The point $[1 : 0]$ corresponds to $k = p^\alpha$ and form the cusp c_∞ of width 1.

Hence we found that:

- for each value of k in $[|0, \lfloor \alpha/2 \rfloor|]$, there are $\phi(\gcd(p^k, p^{\alpha-k}))$ cusps of width $p^{\alpha-2k}$,
- for each value of k in $[|\lfloor \alpha/2 \rfloor + 1, \alpha|]$, there are $\phi(\gcd(p^k, p^{\alpha-k}))$ cusps of width 1.

□

Proposition 20. *Let M, N be two coprime integers. Then*

$$\mathcal{C}(MN) = \mathcal{C}(M) \times \mathcal{C}(N) \ .$$

Proof. Consider the two canonical morphisms

$$\begin{array}{ccc} \mathcal{B}_{0,NM} & \xrightarrow{(g,\chi)} & \mathcal{B}_{0,N} \\ \Big\downarrow{\scriptstyle (f,\phi)} & & \\ \mathcal{B}_{0,M} & & \end{array} \ .$$

From the very definition of these morphisms, the image of a cycle of $y_{0,MN}x_{0,MN}$ by (f, ϕ) (resp. (g, χ)) can only be a cycle of $y_{0,M}x_{0,M}$ (resp. $y_{0,N}x_{0,N}$), possibly of smaller width, but in that case the width of the image divides the width of the original cycle.

Hence the width of the cusp containing the edge $(e_M, e_N) \in E_{0,M} \times E_{0,N}$ is a multiple of $w(e_M)w(e_N)$, where $w(e_M)$ (respectively $w(e_N)$) is the width of the cusp in $\mathcal{B}_{0,M}$ (resp., $\mathcal{B}_{0,N}$) containing e_M (respectively e_N). One actually knows even more, since Proposition 18 and the equality

$$E_{0,MN} = E_{0,M} \times E_{0,N}$$

force it to be exactly $w(e_M)w(e_N)$. That concludes the proof. □

Proposition 20 can be rephrased as the statement that the "width number" function, which associates $|\mathcal{C}(N)|$ to $N \in \mathbb{N}_{>0}$, is multiplicative. Moreover, the reasonning in the proof of Proposition 20 together with Proposition 19 show the following:

Corollary 2. *Let $N > 1$ be an integer. Then*

$$w : \mathcal{C}(N) \to \mathrm{Div}(N) \ ,$$

where $\mathrm{Div}(N)$ *is the set of divisors of N.*

Note that this function is onto if and only if N is square-free. Putting all together, we have proved the following result.

Theorem 2. *Let $N > 2$ be an integer. Then*

$$|\mathcal{C}(N)| = \sum_{d|N} \phi(\gcd(d, \frac{N}{d})) \ .$$

To each d dividing N, there correspond $\phi(\gcd(d, \frac{N}{d}))$ cusps. Writing $N = \prod_i p_i^{\alpha_i}$ and $d = \prod_i p_i^{\beta_i}$, the width of such a cusp is:

$$w(c_{d,k}) = \prod_i \max(1, p_i^{\alpha_i - 2\beta_i}) \ .$$

2.3.4 L-series of the cusps

In this section we will denote $c(\cdot)$ the cusp number function $|\mathcal{C}(\cdot)| : \mathbb{N}_{>0} \to \mathbb{N}_{>0}$.

Proposition 21. *Let $p \in \mathbb{N}$ be a prime number and let $\alpha \in \mathbb{N}_{>0}$. Then:*

$$c(p^{2\alpha+1}) = 2p^\alpha \ .$$

If moreover $\alpha \geq 1$,

$$c(p^{2\alpha}) = p^{\alpha-1}(p+1) \ .$$

Proof. From Theorem 2, and for $k \in \mathbb{N}$

$$c(p^k) = \sum_{0 \leq l \leq k} \phi(\gcd(p^l, p^{k-l}) \ .$$

Since $\phi(p^i) = p^{i-1}(p-1)$, one can write:

$$c(p^{2\alpha+1}) = 2 \sum_{0 \leq k \leq \alpha} p^{k-1}(p-1) = 2 + 2(p-1) \sum_{0 \leq k \leq \alpha-1} p^k = 2 + 2(p-1)\frac{p^\alpha - 1}{p-1} = 2p^\alpha.$$

Mutatis mutandis,

$$c(p^{2\alpha}) = 2 \sum_{0 \leq k \leq \alpha-1} p^{k-1}(p-1) + p^{\alpha-1}(p-1) = 2 + 2(p^{\alpha-1}) - 2 + p^{\alpha-1}(p-1) = p^{\alpha-1}(p+1).$$

□

Definition 15. *The formal L-series associated to the function $c(n)$ is*

$$L(c, s) = \sum_{n \geq 0} \frac{c(n)}{n^s} \ .$$

Since $c(n)$ is multiplicative, one can write $L(c, s)$ as an Euler product

$$L(c, s) = \prod_{p \text{ prime}} L_p(c, s) = \prod_{p \text{ prime}} \sum_{\alpha \geq 0} \frac{c(p^\alpha)}{p^{\alpha s}} \ .$$

For all prime p, and all $s \in \mathbb{C}$ such that

$$|s| > \frac{1}{2} + \frac{e}{2 \ln 2} \ ,$$

the series $L_p(c, s)$ converges absolutely.

Proposition 22. *Let $s \in \mathbb{C}$ satisfying the latter bound. One can rearrange $L_p(c,s)$ as:*

$$L_p(c,s) = L_p(c,s)_e + L_p(c,s)_o = \sum_{\alpha\geq 0} \frac{c(p^{2\alpha})}{p^{2\alpha s}} + \sum_{\alpha\geq 0} \frac{c(p^{2\alpha+1})}{p^{(2\alpha+1)s}} \ ,$$

and the computation yields:

$$L_p(c,s)_e = \frac{p^s + p^{-s}}{p^s - p^{1-s}} \ , \qquad L_p(c,s)_o = \frac{2}{p^s - p^{1-s}} \ .$$

Proof. One readily computes:

$$\begin{aligned} L_p(c,s)_e &= 1 + (1+\frac{1}{p}) \sum_{\alpha\geq 1} \frac{p^\alpha}{p^{2\alpha s}} = 1 + (1+\frac{1}{p}) \sum_{\alpha\geq 1} (p^{1-2s})^\alpha \\ &= 1 + (1+\frac{1}{p})(\frac{p^{1-2s}}{1-p^{1-2s}}) = \frac{1 - p^{1-2s} + p^{1-2s} + p^{-2s}}{1-p^{1-2s}} = \frac{p^s + p^{-s}}{p^s - p^{1-s}} \ , \end{aligned}$$

and similarly

$$L_p(c,s)_o = \frac{2}{p^s} \sum_{\alpha\geq 0} p^{\alpha(1-2s)} = \frac{2}{p^s} \frac{1}{1-p^{1-2s}} = \frac{2}{p^s - p^{1-s}} \ .$$

□

Corollary 3. *The series $L(c,s)$ can be expressed in terms of Riemann's ζ-function:*

$$L(c,s) = \zeta(2s-1)(\frac{\zeta(s)}{\zeta(2s)})^2 \ .$$

Proof. From Proposition 22, for a given prime p, one has:

$$L_p(c,s) = L_p(c,s)_e + L_p(c,s)_o = \frac{p^s + p^{-s}}{p^s - p^{1-s}} + \frac{2}{p^s - p^{1-s}} = \frac{(p^{s/2} + p^{-s/2})^2}{p^s - p^{1-s}} = \frac{(1+p^{-s})^2}{1-p^{1-2s}} \ .$$

Hence

$$L(c,s) = \prod_{p \text{ prime}} \frac{(1+p^{-s})^2}{1-p^{1-2s}}$$

Now $\zeta(s) = \displaystyle\prod_{p \text{ prime}} \frac{1}{1-p^{-s}}$ and $\dfrac{\zeta(s)}{\zeta(2s)} = \displaystyle\prod_{p \text{ prime}} (1+p^{-s})$. □

2.4 Complex structures and Belyĭ maps

In this subsection we discuss analytical aspects of the dessins, realised explicitly as preimages of so-called Belyĭ maps. We follow closely the presentation of [JW16].

2.4.1 The triangle group $\mathrm{PSL}_2(\mathbb{Z}) \simeq \Delta(2,3,\infty)$ and its action on $\mathbb{H}$

The **triangle group** of type (a,b,c) is the group with presentation:

$$\Delta(a,b,c) = \langle X, Y, Z | X^a = Y^b = Z^c = XYZ = 1 \rangle \ . \tag{12}$$

The modular group corresponds to the special case

$$\Delta(2,3,\infty) = \langle S, U, Z | S^2 = U^3 = SUZ = 1 \rangle \simeq \mathrm{PSL}_2(\mathbb{Z}) \ .$$

Consider a hyperbolic triangle T with internal angles $\pi/2$, $\pi/3$ and 0 (for example, the triangle in the hyperbolic plane $\mathbb{H}$ with vertices i, $e^{i\pi/3}$ and ∞). Then, the group generated by the rotations through $2\pi/2$, $2\pi/3$ and 0 about the vertices of this triangle is $\Delta(2,3,\infty)$. Let the **extended triangle group** $\Delta[2,3,\infty]$ be the group generated by the reflections with respect to the sides of T. The half-plane $\mathbb{H}$ is tessellated by the images of T under $\Delta[2,3,\infty]$, and the group $\Delta(2,3,\infty)$ is the subgroup of order 2 in $\Delta[2,3,\infty]$ consisting of the transformations which preserve the orientation.

Consider the following graph embedded in $\mathbb{H}$: let there be a white (respectively, black and red) vertex at each image of i (respectively, $e^{i\pi/3}$ and ∞) under $\Delta(2,3,\infty)$, and an edge for each image of the sides of T under the same group. Now, remove the red vertices and all edges incident to them; this yields a bipartite graph embedded in $\mathbb{H}$. The counterclockwise orientation on $\mathbb{H}$ induces a fat structure on the graph, and the corresponding ABM is $\mathcal{B}_\infty(2,3,\infty)$. By construction, $\mathrm{PSL}_2(\mathbb{Z})$ is the group generated by the rotations about the vertices of the hyperbolic triangle T, and hence naturally appears as the automorphism group of this ABM:

$$\mathrm{Aut}(\mathcal{B}_\infty(2,3,\infty)) \simeq \Delta(2,3,\infty) \simeq \mathrm{PSL}_2(\mathbb{Z}) \ . \tag{13}$$

Since this ABM is regular (because the automorphism group is transitive, for example), $\mathrm{PSL}_2(\mathbb{Z})$ is also the cartographic group of $\mathcal{B}_\infty(2,3,\infty)$.

2.4.2 Complex structure on the surfaces corresponding to the $\mathcal{B}_{0,N}$

Let $N \in \mathbb{N}_{>0}$. Recall that the dessin d'enfant $\mathcal{B}_{0,N}$ is the quotient $\Gamma_0(N)\backslash\mathcal{B}_\infty(2,3,\infty)$, and that it comes with topological surfaces $X_0(N)$ and $Y_0(N)$.

The embedding $\mathcal{B}_\infty(2,3,\infty) \hookrightarrow \mathbb{H}$ induces a complex structure on $X_0(N)$ and $Y_0(N)$, as explained pedagogically in [JW16]. As shown in Figures 9 and 10,each $\mathcal{B}_{0,N}$ corresponds to a fundamental domain for the action of $\Gamma_0(N)$ on $\mathbb{H}$.

The complex structure on the surfaces $X_0(N)$ and $Y_0(N)$ may have torsion (or orbifold) points of order 2 and 3. In terms of Fuchsian groups, each of these torsion points corresponds to an equivalence class of fixed points for some elliptic transformations in $\Gamma_0(N)$. In the bipartite fat graphs, the torsion points of order 2 correspond to the 1-valent white vertices and the torsion points of order 3, to the 1-valent black vertices. Recall that we have computed their number for each N in subsection 2.3.

Example 8. *On the left-hand-side of Figures* 9 *and* 10*, fundamental domains for* $\Gamma_0(3)$ *and* $\Gamma_0(6)$ *obtained with SAGE [S+18] are displayed. In these fundamental domains, the images of the triangle* T *under* $\mathrm{PSL}_2(\mathbb{Z})$ *are in white, those of* T'*, in grey. Colors on the edges label the identifications through which one recovers the topology of the quotient surface* $\Gamma_0(N)\backslash\mathbb{H}$*, but those leading to torsion points (for example, the identification of the two lowermost edges of the fundamental domain shown for* $\Gamma_0(3)$ *is implicit). The corresponding dessins d'enfants (resp.* $\mathcal{B}_{0,3}$ *and* $\mathcal{B}_{0,6}$*) are drawn on the right-hand side of Fig.* 9 *and* 10*.*

2.4.3 Belyĭ's Theorem and dessins d'enfants

The whole theory of dessins d'enfants, and the reason they are related to some number-theoretic questions, relies on the following key theorem [Bel80]. Let X be a compact

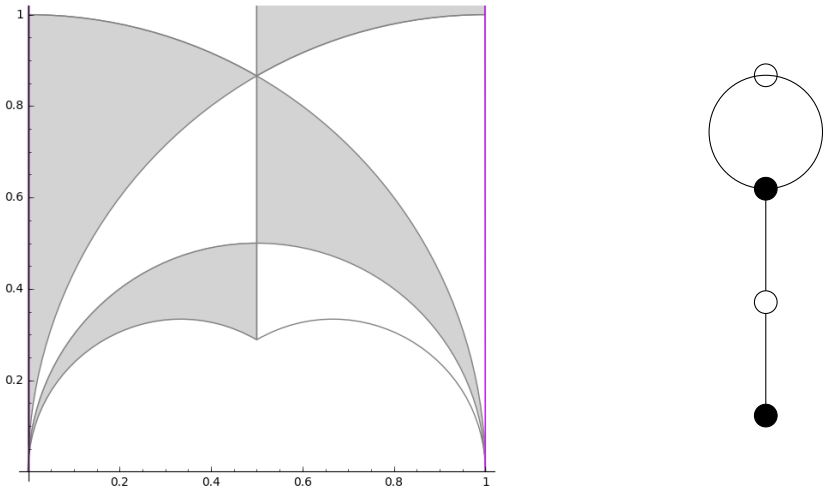


Figure 9: Fundamental domains for $\Gamma_0(3)$ (on the left) and $\mathcal{B}_{0,3}$ (on the right).

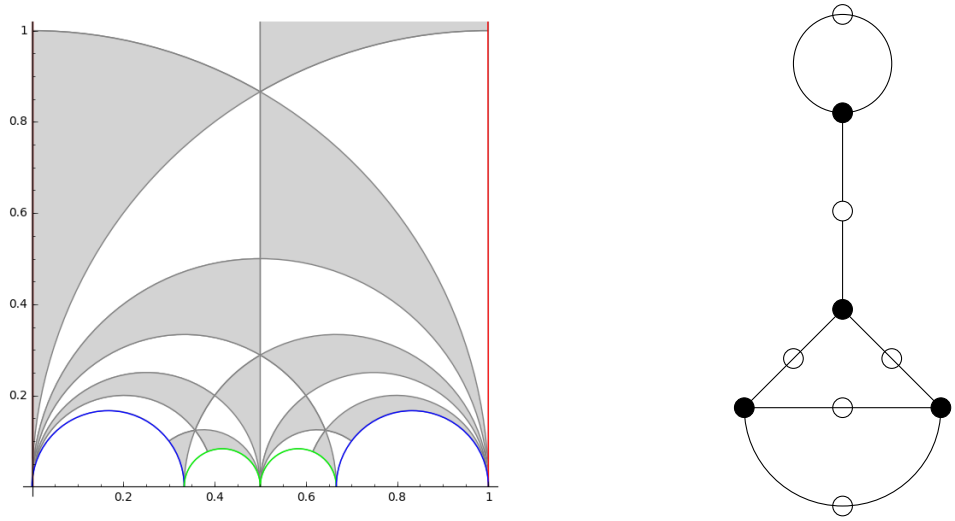


Figure 10: Fundamental domains for $\Gamma_0(6)$ (on the left) and $\mathcal{B}_{0,6}$ (on the right).

Riemann surface. It is a deep and fundamental result that X is biholomorphic to the analytic set of the complex points of a smooth algebraic curve, in a complex projective space $\mathbb{P}^n(\mathbb{C})$ for some $n \in \mathbb{N}_{>0}$.

Let K be a subfield of $\mathbb{C}$. A smooth algebraic curve has **a model over** K if the underlying analytic variety is isomorphic to the zero locus of a finite set of polynomials with coefficients in K, in some affine or projective complex space. Recall that $\overline{\mathbb{Q}}$ is the algebraic closure of the field of rational numbers $\mathbb{Q}$ (equivalently, the field of algebraic numbers).

Theorem 3 (Belyĭ, 1979)**.** *The compact Riemann surface X has a model over $\overline{\mathbb{Q}}$ if and only if there exists a non-constant holomorphic function $\beta : X \to \mathbb{P}^1(\mathbb{C})$ which ramifies over at most three points (which can be chosen to be $0, 1$, and ∞, by considering the action of $\mathrm{PSL}_2(\mathbb{C})$ on $\mathbb{P}^1(\mathbb{C})$ by automorphisms).*

Such a map β is called Belyĭ map. The preimage under β of the real segment $[0, 1] \in \mathbb{P}^1(\mathbb{C})$ is a bipartite graph embedded in X. Since X has a complex structure it is oriented, and this orientation defines a fat structure on this bipartite graph. Hence, any Belyĭ map defines a dessin d'enfant.

Conversely, a dessin d'enfant canonically defines a compact surface on which its underlying graph is embedded. The exact way the dessin d'enfant defines a complex structure on this compact surface is a slight generalisation of the two last paragraphs (again, see [JW16] for more details on this implication). Given a dessin d'enfant, there is always a corresponding Belyĭ map for which the white vertices (respectively, black vertices) are the preimages of 0 (resp., 1) and the edges, the preimages of the segment $[0, 1]$. The explicit expression of this Belyĭ map is in general difficult to derive. One can however motivate its existence as follows.

The dessins d'enfants of type $(2, 3, c)$ yield complex structures built from the hyperbolic triangle T of type $(2, 3, \infty)$. This (open) triangle is conformally equivalent to $\mathbb{H}$ as a consequence of Riemann's open mapping theorem, and a stronger version of the latter even implies that the biholomorphism $J : T \to \mathbb{H}$ can be extended continuously to the boundary ∂T of T, and chosen in such a way that the vertices of T are mapped to $0, 1$ and ∞. Schwarz's reflection principle then asserts that one can extend J to its image T' under the reflection through the edge $[i, e^{i\pi/3}]$, which yields a map $J : (T \cup T') \to \mathbb{P}^1(\mathbb{C})$. This map J is usually called Klein's function or Klein's J-invariant. In what follows we will denote this J-invariant $J_{0,1}$, in order to avoid confusion. Successive applications of the reflection principle indeed further extend J to:

$$J : G\backslash\mathbb{H} \to \mathbb{P}^1(\mathbb{C}) \ , \tag{14}$$

for any subgroup $G < \mathrm{PSL}_2(\mathbb{Z})$, and this J can even be continued on the compactification of $G\backslash\mathbb{H}$ (with some help from the removable singularity theorem).

In the end, any subgroup of $G < \mathrm{PSL}_2(\mathbb{Z})$ of finite index (e.g., a $\Gamma_0(N)$) gives rise to a complex surface with cusps, with Fuchsian model $G\backslash\mathbb{H}$. This surface can be compactified by adding a point at each cusp, and comes with a Belyĭ map obtained from Klein's invariant $J_{0,1}$ through the reflection principle. Belyĭ's theorem then states that the algebraic curve defined by such a dessin d'enfant always has a model over a number field.

In fact, it is a classical result that the algebraic curves $Y_0(N)$ and $X_0(N)$, for $N \in \mathbb{N}$, have a model over $\mathbb{Q}$, even if their defining equation over $\mathbb{Q}$ is in general hard to derive. The complete projective algebraic curve $X_0(N)$ corresponding to $\Gamma_0(N)$ is usually called the *(compact) classical modular curve*. It satisfies a polynomial equation with rational coefficients

$$\Phi(x, y) = 0$$

such that $(x, y) = (J(\tau), J(N\tau))$ is a point of the curve, with J the *usual* Klein's function.

2.4.4 Genus formula

For each dessin $\mathcal{B}_{0,N}$ we have a complete description of the set of torsion points of order 2 and 3, the set of cusps, and their width. Moreover we know that the map

$$X_0(N) \to \mathbb{P}^1(\mathbb{C})$$

induced by reflection principle on Klein's invariant $J_{0,1}$ is the Belyĭ map corresponding to this dessin $\mathcal{B}_{0,N}$. This map ramifies at the vertices and the cusps. The ramification order is the valency for a vertex (or the width for a cusp). We now have enough data

to compute the genus of $X_0(N)$ for all $N \in \mathbb{N}_{>0}$ using Riemann-Hurwitz formula. This gives the following.

Theorem 4. *Let $N \in \mathbb{N}_{>0}$, $|E_{0,N}| = N\prod_{p|N}(1+p^{-1})$, and $\nu_2(N)$ (resp., $\nu_3(N)$) the number of torsion points of order 2 (resp., 3) of the dessin $\mathcal{B}_{0,N}$. Let $c_w(N)$ be the number of cusps of width w in $\mathcal{B}_{0,N}$. Then:*

$$\chi(X_0(N)) = 2|E_{0,N}| - \frac{1}{2}(|E_{0,N}| - \nu_2(N)) - \frac{2}{3}(|E_{0,N}| - \nu_3(N)) - \sum_{w\geq 1} c_w(N)(w-1) \ ,$$

where $\chi(X_0(N))$ is the Euler characteristic of $X_0(N)$.

Corollary 4. *Let p be a prime number, and $g(p)$ the genus of $X_0(p)$. Then:*

$$\frac{p-13}{12} \leq g(p) \leq \frac{p+1}{12} \ .$$

Proof. For p prime, $0 \leq \nu_2(p) \leq 2$ and $0 \leq \nu_3(p) \leq 2$, and there are only two cusps: c_0 of width p and c_1 of width 1. Hence, applying Theorem 4 one gets:

$$\frac{1}{6}(11-p) \leq \chi(X_0(p)) \leq \frac{1}{6}(25-p) \ ,$$

and $\chi(X_0(p)) = 2 - 2g(X_0(p))$ gives the desired bounds. □

Some interesting properties of the sequence of genera of the classical modular curves, like bounds, modularity properties and densities are investigated in [CWZ00].

2.4.5 Moduli problem of level-N structures on elliptic curves

The classical modular curves $Y_0(N)$ are known to solve a moduli problem.

Let E be an elliptic curve over a perfect field k, typically the field of rational numbers $\mathbb{Q}$, and let $N \in \mathbb{N}_{>0}$. A cyclic subgroup of E of order N is a Zariski-closed subset S of E such that $S(\bar{k})$ is a cyclic subgroup of $E(\bar{k})$ of order N, where $\bar{k}$ is the algebraic closure of k. Consider the pairs (E, S) up to isomorphism, where

$$f : (E, S) \to (E', S')$$

is an isomorphism if $f : E \to E'$ an isomorphism such that $f(S) = S'$. It is the moduli problem we are interested in, and has the modular curve $Y_0(N)$ as solutions. See [Mil97] for a more detailed discussion.

Over the complex numbers, the elliptic curves correspond to the projective lattices in the complex plane. A projective lattice L_1 in a two dimensional real vector space, and modulo $\mathrm{PSL}_2(\mathbb{Z})$, corresponds to an elliptic curve E_1. The projective lattices N-hyperdistant from L_1 correspond in turn to the cyclic subgroups of E of order N. Hence the dessins d'enfants describe the part of the structure of the moduli spaces $Y_0(N)$ which concerns the *cyclic subgroups of order N*, while the complex surface associated with those dessins brings the *moduli space of complex structures* to the picture.

2.5 Hauptmoduln and Belyĭ maps

We now focus on the special class of Hecke congruence subgroups that appear in the Monstrous Moonshine correspondence [CN79], namely, those of genus 0.

2.5.1 Hauptmoduln for genus zero algebraic curves

Let $\tilde{X}$ be an analytic projective irreducible curve embedded in some $\mathbb{P}^n(\mathbb{C})$. There exists a non-singular model X of $\tilde{X}$ which has the same field of meromorphic functions as X:

$$\mathcal{M}_X = \mathcal{M}_{\tilde{X}} \ .$$

It is a classical result (see for example [Ful89]) that *over the complex numbers*, the following holds:

$$\tilde{X} \text{ is rational} \qquad \Leftrightarrow \qquad X \text{ is biholomorphic to } P^1(\mathbb{C}),$$

that is, over $\mathbb{C}$ the curve $\tilde{X}$ is rational if and only if X has genus zero. Whenever it is the case, $\tilde{X}$ can be parametrised by a rational function of a single variable (which lives on $\mathbb{P}^1$).

Definition 16. *Let X be a genus-zero Riemann surface. Its field of meromorphic functions $\mathcal{M}_X$ is the field of rational fractions in a single meromorphic function over X. Such a function is called a* **Hauptmodul** *(or principal modulus) for X.*

2.5.2 Belyĭ maps and replication Formulæ for J

From now on, for all $N \in \mathbb{N}$ let $X_0(N)$ be the analytic complex curve $X_0(N)(\mathbb{C})$.

Choice of a coordinate Exactly 15 classical modular curves $X_0(N)$ are of genus zero (and hence rational): those corresponding to

$$N \in \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12, 13, 16, 18, 25\} \ .$$

For all N in this set, there is a conformal isomorphism (whose existence is provided by the open-mapping theorem):

$$J_{0,N} : X_0(N) \to \mathbb{P}^1(\mathbb{C}) \ .$$

The function $J_{0,N}$ is a Hauptmodul for the curve $X_0(N)$:

$$\begin{array}{ccc} X_0(N) & \to & \mathbb{P}^1(C) \\ \tau & \mapsto & J_{0,N}(\tau) =: t \end{array}$$

The analytic curve $X_0(N)$ is the (smoothened compactification of the) quotient of the upper-half plane under the action of $\Gamma_0(N)$. Every choice of fundamental domain for $\Gamma_0(N)$ in $\mathbb{H}$ defines a chart on $X_0(N)$, on which $J_{0,N}$ can be explicitly expressed in terms of Dedekind's η (see table 3 of [CN79]).

Belyĭ maps Recall that Klein's invariant $J_{0,1}$ defines a branched cover

$$\beta_{0,N} : X_0(N) \to \mathbb{P}^1(\mathbb{C})$$

which ramifies only over 1, 0 and ∞, with ramification order dividing 2 over 1, and 3 over 0. Since $X_0(N)$ is biholomorphic to $\mathbb{P}^1(\mathbb{C})$, this map can be expressed as:

$$\beta_{0,N} : \mathbb{P}^1(\mathbb{C}) \to \mathbb{P}^1(\mathbb{C}) \ .$$

It is a Belyĭ map which corresponds to the dessin d'enfant $\mathcal{B}_{0,N}$.

This map $\beta_{0,N}$ is a rational function of t, by definition of a Hauptmodul. Note that:

1. The set of preimages of 0 is the set of black vertices of the corresponding dessin. The multiplicity of a root is the valence of the corresponding vertex. The set of poles is the set of faces, and the multiplicity of a pole is the width of the corresponding cusp. The set of preimages of 1 is the set of white vertices, and the multiplicity of a preimage of 1 is the valence of the corresponding vertex.

2. Let $N \in \mathbb{N}_{>0}$. Since the dessin d'enfant $\mathcal{B}_{0,N}$ is of type $(2,3,N)$, the multiplicities of the roots of the numerator of $\beta_{0,N}$ are either one or three, and the multiplicities of the preimagesof 1, either one or two.

3. The classical modular curves $X_0(N)$ all have a model over $\mathbb{Q}$: they can be defined by a polynomial equation
$$\Phi_N(X,Y) = 0$$
where $\Phi_N \in \mathbb{Q}[X,Y]$, and such that $(J(\tau), J(N\tau))$ is a point of $X_0(N)$. The function $J(\tau)$ is is a rational fraction of the Hauptmodul $t = J_{0,N}(\tau)$, with rational (equivalently, integer) coefficients: $J(\tau) = \beta_{0,N}(t)$.

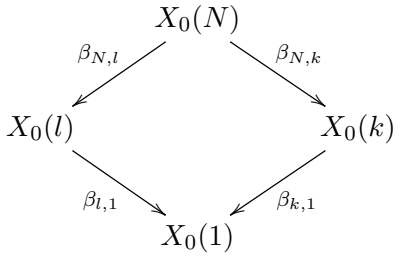
N	$J(\tau) = \beta_{0,N}(t)$ (Belyĭ map)
1	t
2	$\frac{(t+256)^3}{1728t^2}$
3	$\frac{27(t+9)^3(t+1)}{1728t^3}$
4	$\frac{16(t^2+16t+16)^3}{1728(t+1)t^4}$
5	$\frac{(t^2+250t+3125)^3}{1728t^5}$
6	$\frac{(2t+3)^3(8t^3+252t^2+486t+243)^3}{1728t^6(8t+9)^3(t+1)^2}$
7	$\frac{(t^2+13t+49)(t^2+245t+2401)^3}{1728t^7}$
8	$\frac{4(t^4+64t^3+320t^2+512t+256)^3}{1728t^8(t+2)^2(t+1)}$
9	$\frac{3(t+3)^3(t^3+81t^2+243t+243)^3}{1728t^9(t^2+3t+3)}$
10	$\frac{(t^6+260t^5+6400t^4+64000t^3+320000t^2+800000t+800000)^3}{1728t^{10}(t+5)^5(t+4)^2}$
12	$\frac{(3t^6+252t^5+1464t^4+3456t^3+4032t^2+2304t+512)^3(3t^2+12t+8)^3}{1728t^{12}(3t+4)^4(t+2)^3(t+1)^3(3t+2)}$
13	$\frac{(t^4+247t^3+3380t^2+15379t+28561)^3(t^2+5t+13)}{1728t^{13}}$
16	$\frac{2(t^8+128t^7+1408t^6+6656t^5+17664t^4+28672t^3+28672t^2+16384t+4096)^3}{1728t^{16}(t+2)^4(t^2+2t+2)(t+1)}$
18	$\frac{(t^9+9t^8+270t^7+1728t^6+5832t^5+13122t^4+21870t^3+26244t^2+19683t+6561)^3(t^3+3t^2+9t+9)^3}{1728t^{18}(t+3)^9(t^2+3t+3)^2(t^2+3)^2(t+1)}$
25	$\frac{(t^{10}+250t^9+4375t^8+35000t^7+178125t^6+631250t^5+1640625t^4+3125000t^3+4296875t^2+3906250t+1953125)^3}{1728t^{25}(t^4+5t^3+15t^2+25t+25)}$

Figure 11: These explicit expressions of the Belyĭ maps have been obtained from those in [VH], through $\mathrm{PSL}_2(\mathbb{C})$-rotations of t. It is an interesting fact that the the coefficients appearing in these $\beta_{0,N}$ (for these choices of t) are not only integer, but positive integers. We are not aware of any explanation of this fact in the litterature.

Divisibility relations Let $N \in \mathbb{N}$, and let d be a divisor of N. Since there exists a canonical projection:
$$\mathcal{B}_{0,N} \to \mathcal{B}_{0,k} \ ,$$

the map $J_{0,k}$ defines a function on $X_0(N)$ (through the reflection principle). Again by definition of a Hauptmodul, the induced $J_{0,k}$ is rational fraction of $J_{0,N}$.

Let $k|N$ and $l|k$. The following diagram commutes.



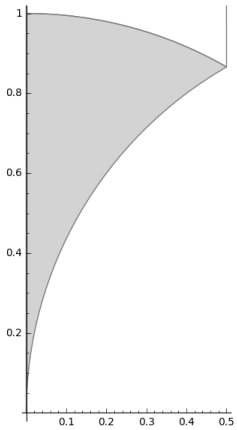
3 Genus zero Hecke groups

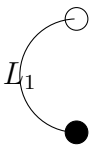
We tabulate fundamental domains, the dessins and the cusps (as cycles of projective lattices) of the 15 genus zero Hecke subgroups, which are exactly the Hecke subgroups of $\mathrm{PSL}_2(\mathbb{Z})$ appearing in the moonshine correspondence.

In the simplest cases (up to $N = 9$), on each edge in the dessin we write the name of the corresponding projective lattice (following the rules described in Appendix A). For $N > 9$ we only write the name of a single projective lattice in each cusp directly on the graph, to avoid being too cumbersome. However, the knowledge of where this projective lattice sits on the graph together with the tabulation of the cusps on the side is enough to keep track of which lattice corresponds to which edge in the dessin. We leave to the reader to check and get familiar with this general rule in the 9 first cases, where the correspondence edge/projective lattice is completely explicit.

$\Gamma_0(1)$

The index in $\mathrm{PSL}_2(\mathbb{Z})$ is 1.

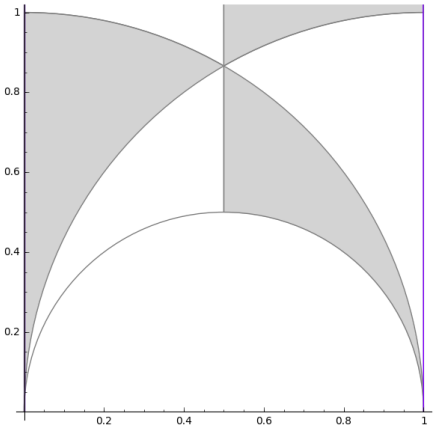


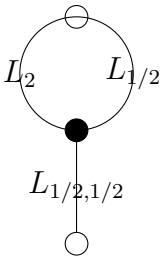


Cusp	Representative	Width
$\{[0:1]\} = \{L_1\}$	∞	1

$\Gamma_0(2)$

The index in $\mathrm{PSL}_2(\mathbb{Z})$ is 3.

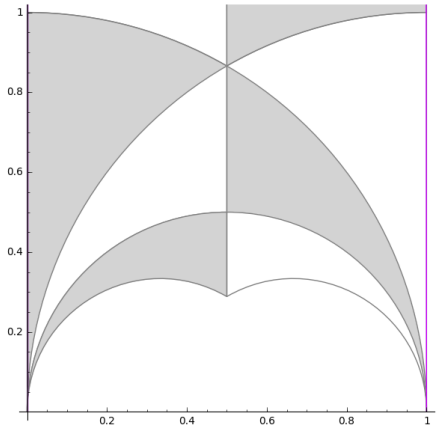


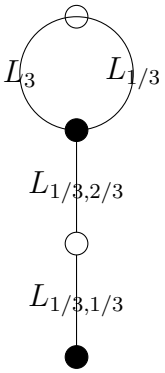


Cusp	Representative	Width
$([0:1],[1:1]) = (L_2, L_{1/2,1/2})$	0	2
$([1:0]) = (L_{1/2})$	∞	1

$\Gamma_0(3)$

The index in $\mathrm{PSL}_2(\mathbb{Z})$ is 4.

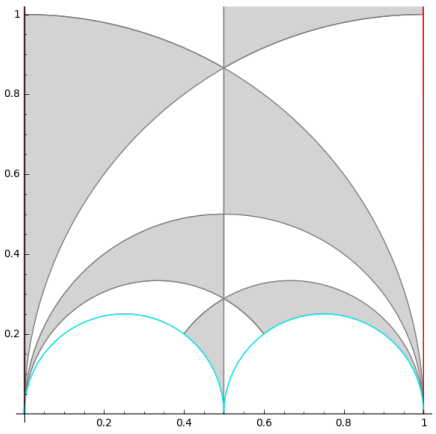


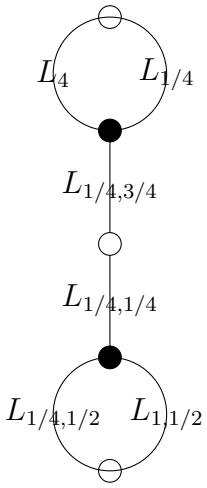


Cusp	Representative	Width
$([0:1],[1:1],[2:1]) = (L_3, L_{1/3,1/3}; L_{1/3,2/3})$	0	3
$([1:0]) = (L_{1/3})$	∞	1

$\Gamma_0(4)$

The index in $\mathrm{PSL}_2(\mathbb{Z})$ is 6.

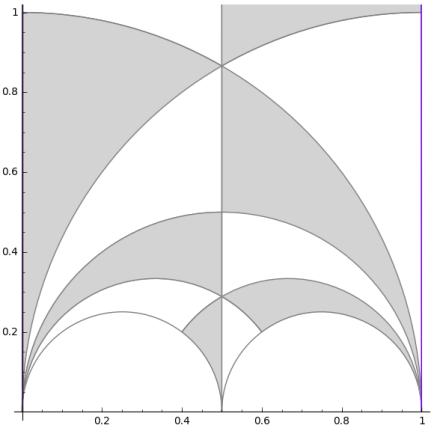


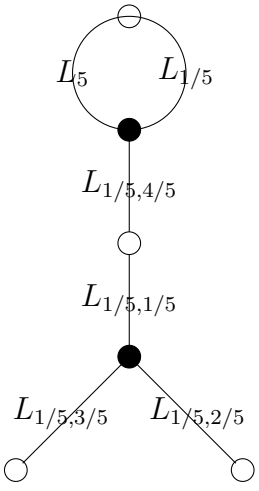


Cusp	Representative	Width
$([0:1],[1:1],[2:1],[3:1]) = (L_4, L_{1/4,1/4}, L_{1,1/2}, L_{1/4,3/4})$	0	4
$[1:2] = L_{1/4,1/2}$	$1/2$	1
$[1:0] = L_{1/4}$	∞	1

$\Gamma_0(5)$

The index in $\mathrm{PSL}_2(\mathbb{Z})$ is 6.

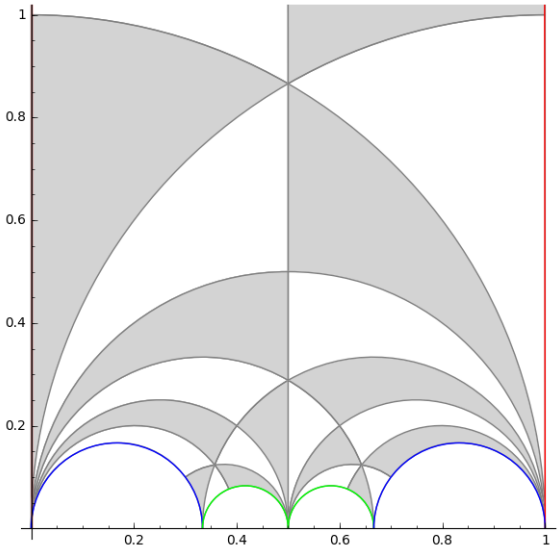


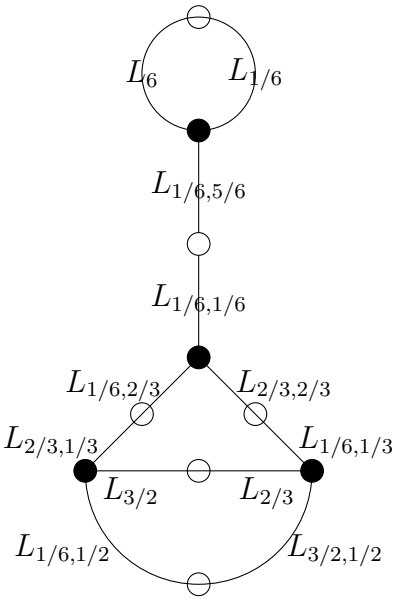


Cusp	Representative	Width
$([0:1],...,[4:1]) = (L_5, L_{1/5,1/5}, L_{1/5,3/5}, L_{1/5,2/5}, L_{1/5,4/5})$	0	5
$([1:0]) = (L_{1/5})$	∞	1

$\Gamma_0(6)$

The index in $\mathrm{PSL}_2(\mathbb{Z})$ is 12.

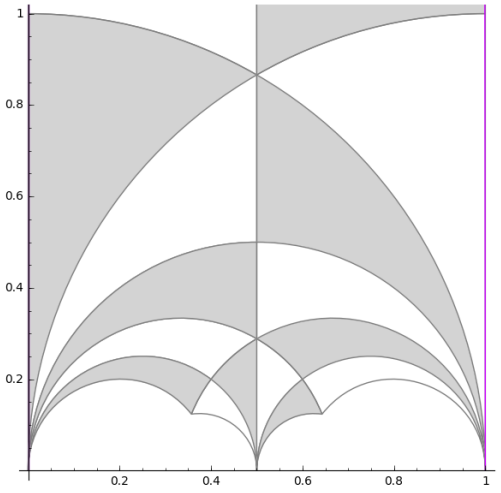


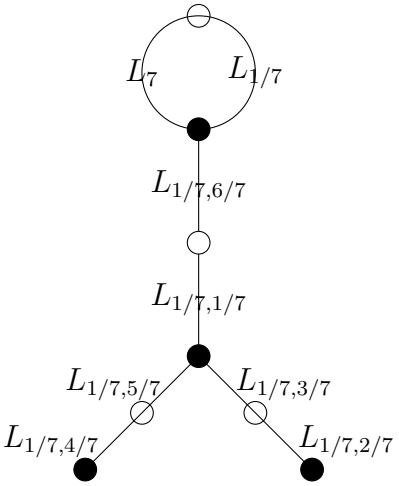


Cusp	Representative	Width
$([0:1],...,[5:1]) = (L_6, L_{1/6,1/6}, L_{2/3,1/3}, L_{3/2,1/2}, L_{2/3,2/3}, L_{1/6,5/6})$	0	6
$([1:3],[2:3]) = (L_{1/6,1/2}, L_{2/3})$	1/3	2
$([1:2],[3:2],[5:2]) = (L_{1/6,1/3}, L_{3/2}, L_{1/6,2/3})$	1/2	3
$([1:0]) = (L_{1/6})$	∞	1

$\Gamma_0(7)$

The index in $\mathrm{PSL}_2(\mathbb{Z})$ is 8.

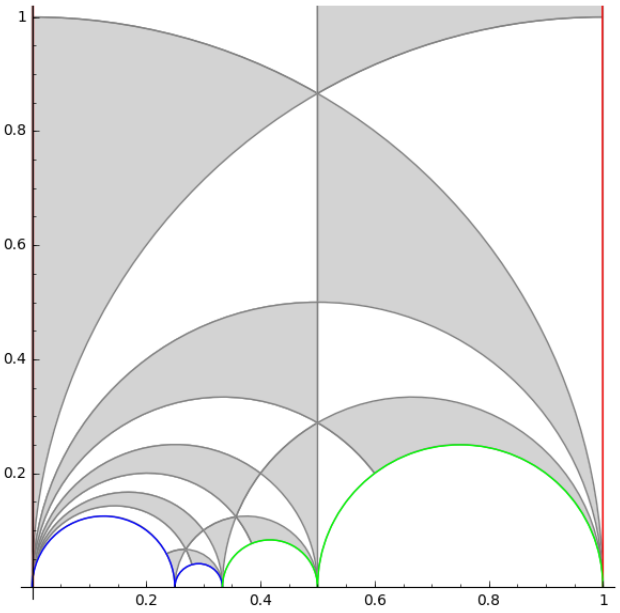


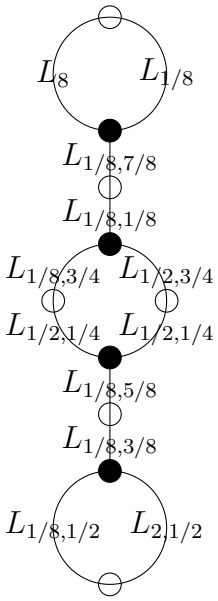


Cusp	Representative	Width
$([0:1],...,[6:1]) =$ $(L_7, L_{1/7,1/7}, L_{1/7,4/7}, L_{1/7,5/7}, L_{1/7,2/7}, L_{1/7,3/7}, L_{1/7,6/7})$	0	7
$([1:0]) = (L_{1/7})$	∞	1

$\Gamma_0(8)$

The index in $\mathrm{PSL}_2(\mathbb{Z})$ is 12.

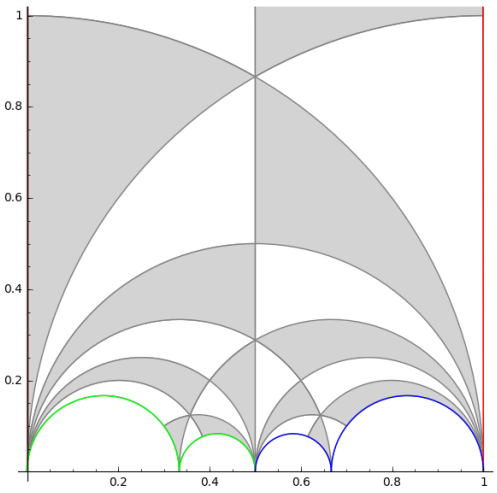


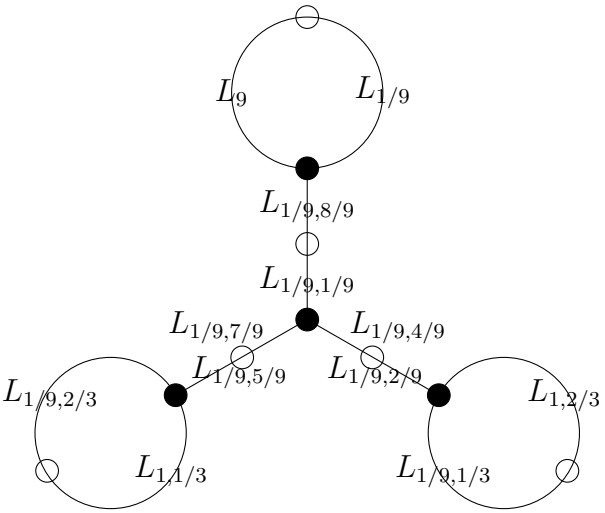


Cusp	Representative	Width
$([0:1],...,[7:1]) =$ $(L_8, L_{1/8,1/8}, L_{1/2,1/4}, L_{1/8,3/8}, L_{2,1/2}, L_{1/8,5/8}, L_{1/2,3/4}, L_{1/8,7/8})$	0	8
$([1:4]) = (L_{1/8,1/2})$	1/4	1
$([1:2],[1:6]) = (L_{1/2,1/4}, L_{1/8,3/4})$	1/2	2
$([1:0] = (L_{1/8}))$	∞	1

$\Gamma_0(9)$

The index in $\mathrm{PSL}_2(\mathbb{Z})$ is 12.

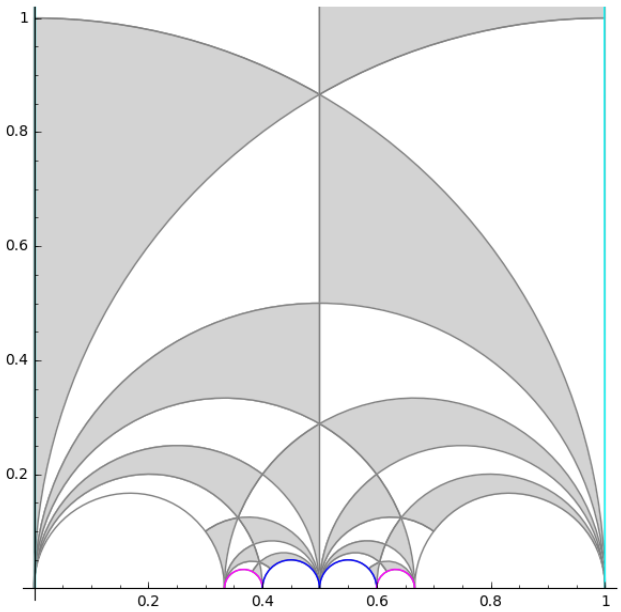


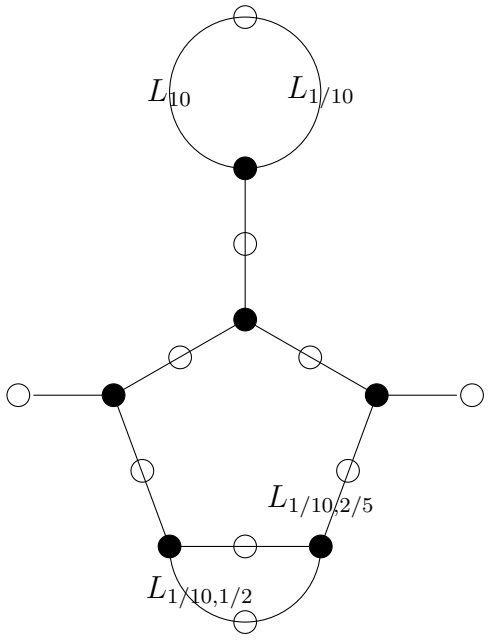


Cusp	Representative	Width
$([0:1],...,[8:1]) = (L_9, L_{1/9,1/9}, L_{1/9,5/9}, L_{1,1/3}, L_{1/9,7/9}, L_{1/9,2/9}, L_{1,2/3}, L_{1/9,4/9}, L_{1/9,8/9})$	0	9
$([1:6]) = (L_{1/9,2/3})$	1/3	1
$([1:3]) = (L_{1/9,1/3})$	2/3	1
$([1:0]) = (L_{1/9})$	∞	1

$\Gamma_0(10)$

The index in $\mathrm{PSL}_2(\mathbb{Z})$ is 18.

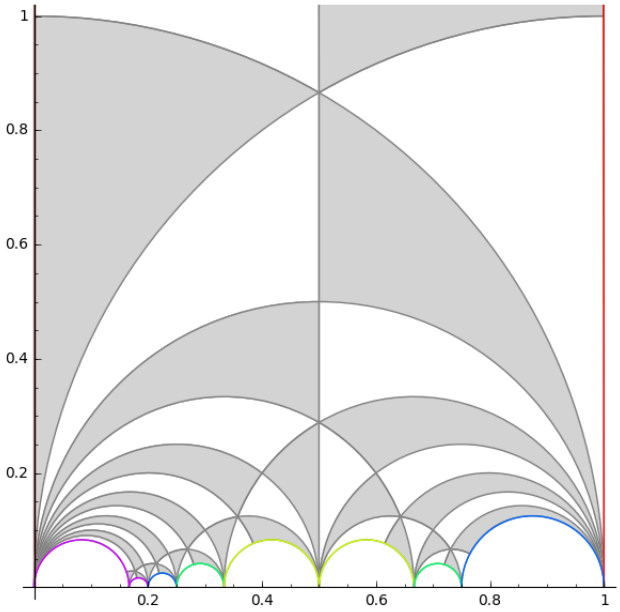


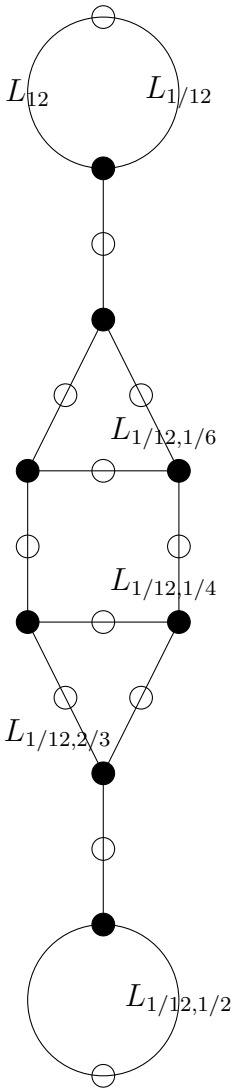


Cusp	Representative	Width
$([0:1],...,[8:1]) = (L_{10}, L_{1/10,1/10}, L_{2/5,1/5}, L_{1/10,7/10}, L_{2/5,3/5}, L_{5/2,1/2}, L_{2/5,2/5}, L_{1/10,3/10}, L_{2/5,4/5}, L_{1/10,9/10}$	0	10
$([1:5],[2:5]) = (L_{1/10,1/2}, L_{2/5})$	$1/3$	2
$([1:2],[1:4],[5:2],[1:6],[1:8]) = (L_{1/10,1/5}, L_{1/10,2/5}, L_{5/2}, L_{1/10,3/5}, L_{1/10,4/5})$	$1/2$	5
$([1:0]) = (L_{1/10})$	∞	1

$\Gamma_0(12)$

The index in $\mathrm{PSL}_2(\mathbb{Z})$ is 24.

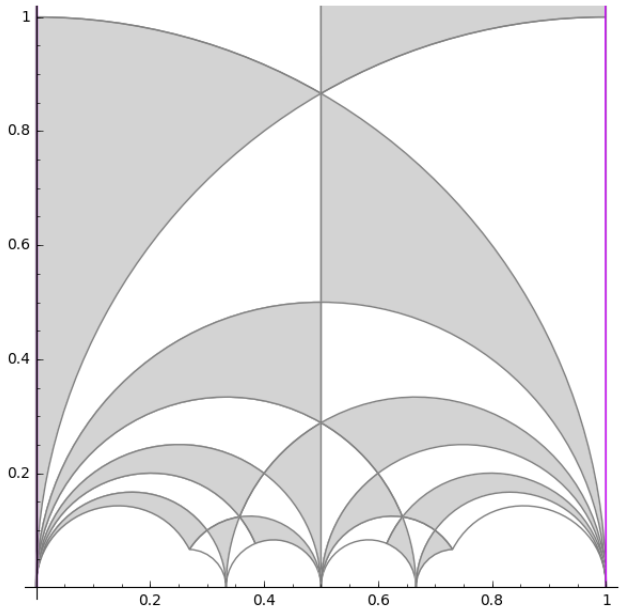


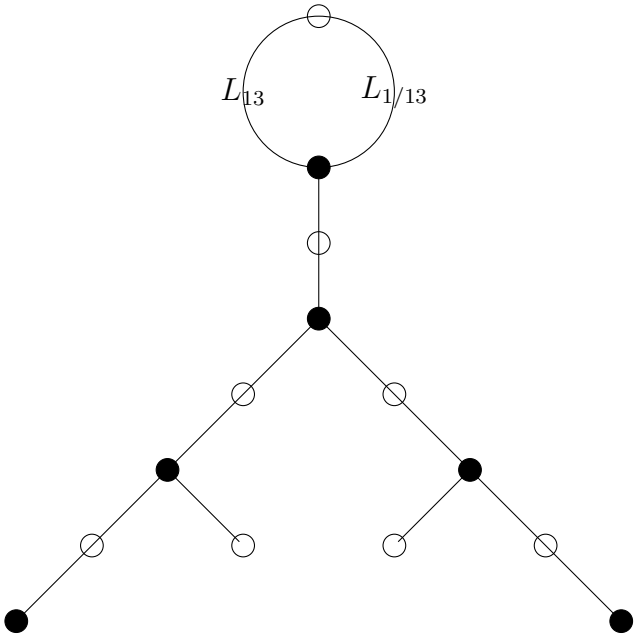


Cusp	Representative	Width
$([0:1],...,[11:1]) = (L_{12}, L_{1/12,1/12}, L_{1/3,1/6}, L_{3/4,1/4}, L_{4/3,1/3}$ $L_{1/12,5/12}, L_{3,1/2}, L_{1/12,7/12}, L_{4/3}, L_{2/3}, L_{3/4,3/4}, L_{1/3,5/6}, L_{1/12,11/12})$	0	12
$([1:6]) = (L_{1/12,1/2})$	1/6	1
$([1:8],[3:8],[1:4]) = (L_{1/12,2/3}, L_{3/4}, L_{1/12,1/3})$	1/4	3
$([1:9],[2:9],[1:3],[4:3]) = (L_{1/12,3/4}, L_{1/3,1/2}, L_{1/12,1/4}, L_{4/3})$	1/3	4
$([1:2],[3:2],[5:2]) = (L_{1/12,1/6}, L_{3/4,1/2}, L_{1/12,5/6})$	1/2	3
$([1:0]) = (L_{1/12})$	∞	1

$\Gamma_0(13)$

The index in $\mathrm{PSL}_2(\mathbb{Z})$ is 14.

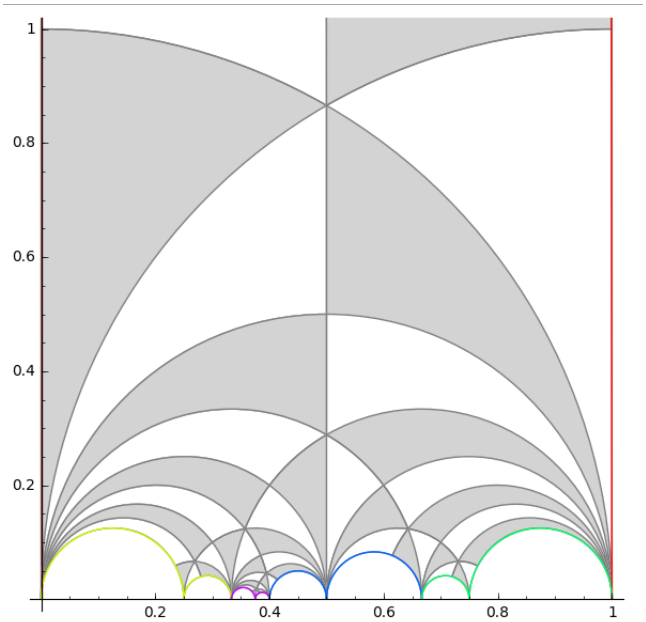


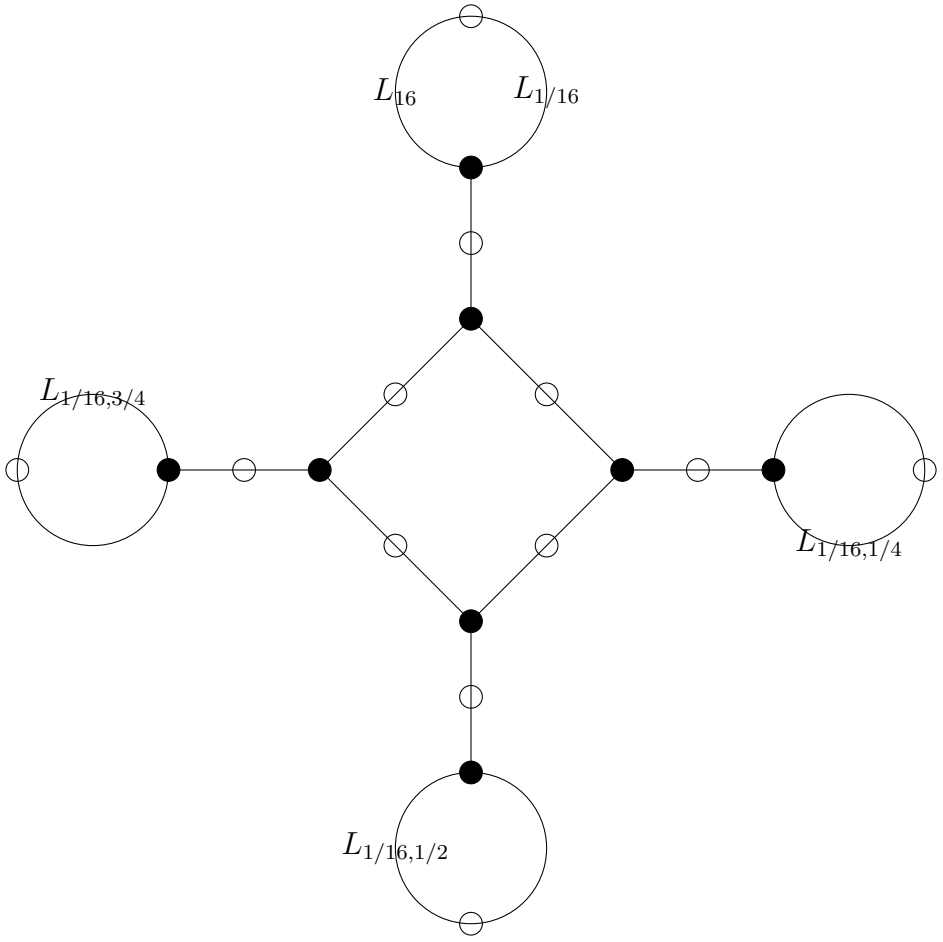


Cusp	Representative	Width
$([0:1],...,[12:1]) = (L_{13}, L_{1/13,1/13}, L_{1/13,7/13}, L_{1/13,9/13}, L_{1/13,10/13}, L_{1/13,8/13}, L_{1/13,11/13}, L_{1/13,2/13}, L_{1/13,5/13}, L_{1/13,3/13}, L_{1/13,4/13}, L_{1/13,6/13}, L_{1/13,12/13})$	0	13
$([1:0]) = (L_{1/13})$	∞	1

$\Gamma_0(16)$

The index in $\mathrm{PSL}_2(\mathbb{Z})$ is 24.

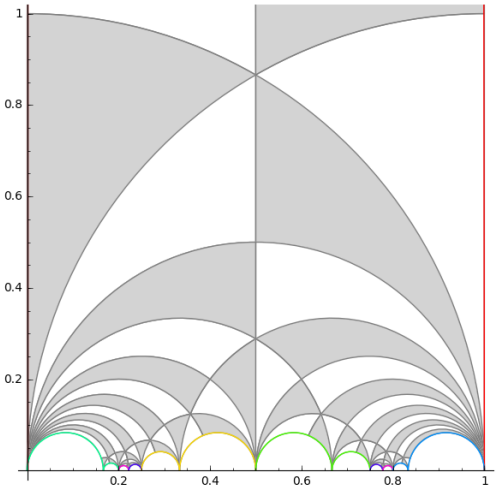


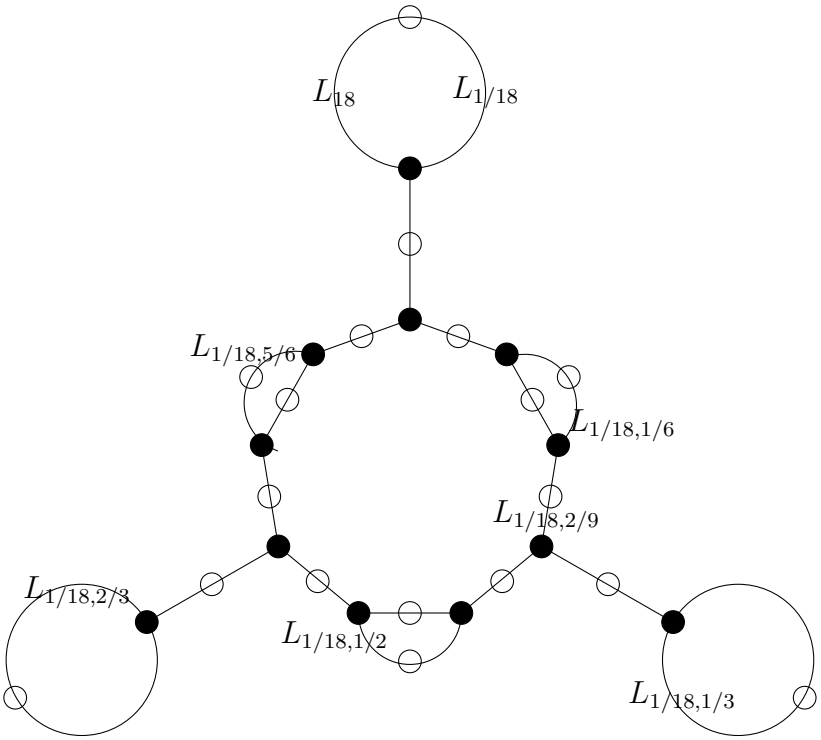


Cusp	Representative	Width
$([0:1],...,[15:1]) = (L_{16}, L_{1/16,1/16}, L_{1/4,1/8}, L_{1/16,11/16}, L_{1,1/4}, L_{1/16,13/16}, L_{1/4,3/8}, L_{1/16,7/16}, L_{4,1/2}, L_{1/16,9/16} L_{1/4,5/8}, L_{1/16,3/16}, L_{1,3/4}, L_{1/16,5/16}, L_{1/4,7/8}, L_{1/16,15/16})$	0	16
$([1:4]) = (L_{1/16,1/4})$	$1/4$	1
$([1:8]) = (L_{1/16,1/2})$	$3/8$	1
$([1:2],[3:2],[5:2],[7:2]) = (L_{1/16,1/8}, L_{1/16,3/8}, L_{1/16,5/8}, L_{1/16,7/8})$	$1/2$	4
$([1:12]) = (L_{1/16,3/4})$	$3/4$	1
$([1:0]) = (L_{1/16})$	∞	1

$\Gamma_0(18)$

The index in $\mathrm{PSL}_2(\mathbb{Z})$ is 36.

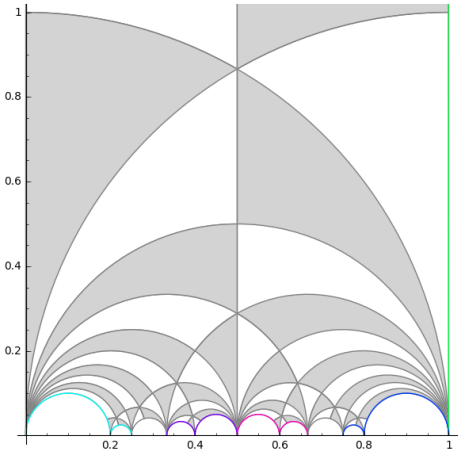


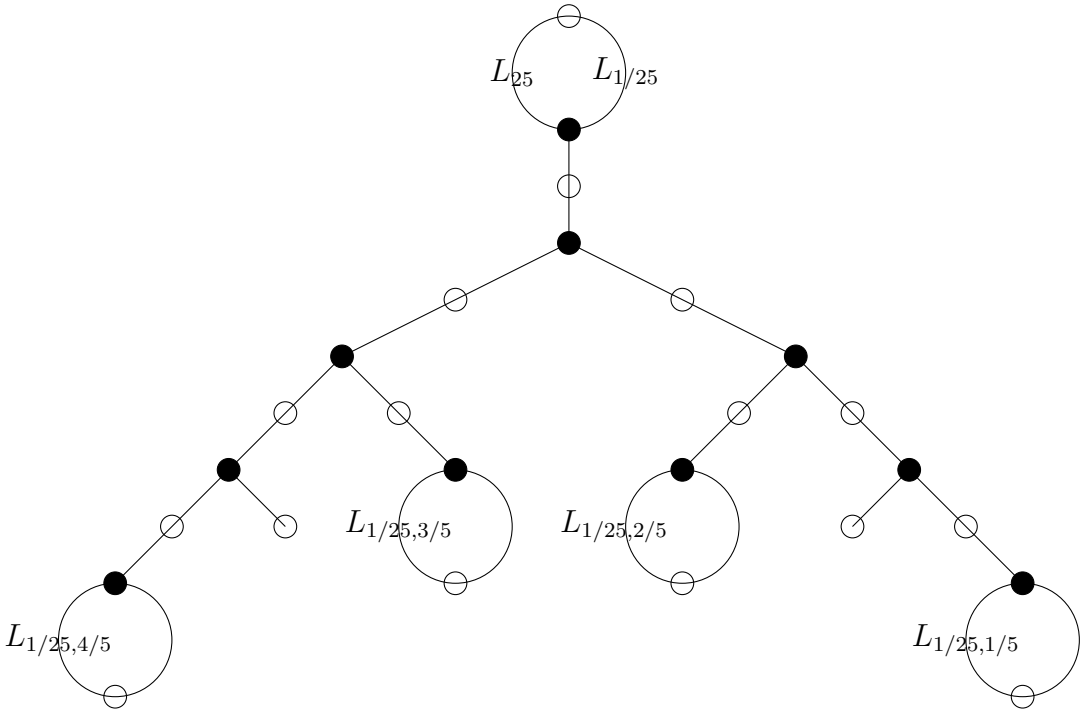


Cusp	Representative	Width
$([0:1],...,[18:1]) = (L_{18}, L_{1/18,1/18}, L_{2/9,1/9}, L_{1/2,1/6}, L_{2/9,5/9}, L_{1/18,11/18}, L_{2,1/3}, L_{1/18,13/18}, L_{2/9,7/9}, L_{9/2,1/2}, L_{2/9,2/9} L_{1/18,5/18}, L_{2,2/3}, L_{1/18,7/18}, L_{2/9,4/9}, L_{1/2,5/6}, L_{2/9,8/9}, L_{1/18,17/18})$	0	18
$([1:12]) = (L_{1/18,2/3})$	1/6	1
$([1:9],[2:9]) = (L_{1/18,1/2}, L_{2/9})$	2/9	2
$([1:2],[3:2],[5:2],[7:2],[9:2],[11:2],[13:2],$ $[15:2],[17:2]) = (L_{1/18,1/9}, L_{1/2,1/3}, L_{1/18,2/9}, L_{1/18,4/9}, L_{9/2},$ $L_{1/18,5/9}, L_{1/18,7/9}, L_{1/2,2/3}, L_{1/18,8/9})$	1/4	9
$([2:3],[5:3]) = (L_{2/9,1/3}, L_{1/18,5/6})$	1/3	2
$([1:3],[4:3]) = (L_{1/18,1/6}, L_{2/9,2/3})$	2/3	2
$([1:6]) = (L_{1/18,1/3})$	5/6	1
$([1:0]) = (L_{1/18})$	∞	1

$\Gamma_0(25)$

The index in $\mathrm{PSL}_2(\mathbb{Z})$ is 30.





Cusp	Representative	Width
$([0:1],...,[24:1]) = (L_{25}, L_{1/25,1/25}, L_{1/25,13/25}, L_{1/25,17/25}, L_{1/25,19/25}, L_{1,1/5}, L_{1/25,21/25}, L_{1/25,18/25}, L_{1/25,22/25}, L_{1/25,14/25}, L_{1,3/5}, L_{1/25,16/25}, L_{1/25,23/25}, L_{1/25,2/25}, L_{1/25,9/25}, L_{1,2/5}, L_{1/25,11/25}, L_{1/25,3/25}, L_{1/25,7/25}, L_{1/25,4/25}, L_{1,4/5}, L_{1/25,6/25}, L_{1/25,8/25}, L_{1/25,12/25}, L_{1/25,24/25})$	0	25
$([1:20]) = (L_{1/25,4/5})$	1/5	1
$([1:15]) = (L_{1/25,3/5})$	2/5	1
$([1:10]) = (L_{1/25,2/5})$	3/5	1
$([1:5]) = (L_{1/25,1/5})$	4/5	1
$([1:0]) = (L_{1/25})$	∞	1

**

A Lattices and Hecke groups

We present here the approach to arithmetic groups developped by Conway in [Con96], in terms of their action on lattices. The modular group $\mathrm{PSL}_2(\mathbb{Z})$ and its Hecke congruence subgroups $(\Gamma_0(N))_{N\geq 1}$ naturally appear as stabilisers in $\mathrm{PGL}_2^+(\mathbb{Q})$ of a pair of projective lattices in a 2-dimensional real vector space.

We closely follow the first sections [Dun09] which fit our purposes well, and even restrict to two dimensions. The article [Pla19] ties a link between this and non-commutative geometry systems as developed by Marcolli and Connes.

A.1 Linear transformations

Let V be a two-dimensional vector space over $\mathbb{R}$, with a basis (e^1, e^2) refered to as the **reference basis** is what follows, and fixed throughout our paper. A vector $v \in V$ is written as a row of two coordinates (generically denoted v_1 and v_2) with the basis specified when needed. For example, in the reference basis

$$v = (v_1\ v_2) = \sum_{i=1}^{2} v_i e^i \ . \tag{15}$$

Definition 17. *Let f^1, f^2 be two vectors in V. The pair (f^1, f^2) is an oriented basis of V if $f^1 \wedge f^2$ is a strictly positive multiple of $e^1 \wedge e^2$. Let $\mathcal{B}^+ \subset V^2$ be the subset of oriented bases. In what follows, oriented bases $(f^1, f^2) \in \mathcal{B}^+$ are written as 2×1 matrices of vectors in V.*

The ring $\mathrm{End}(V)$ of endomorphisms of V acts naturally on V on the right:

$$\begin{array}{rcl} V \times \mathrm{End}(V) & \to & V \\ (v, A) & \mapsto & v \cdot A \end{array} \ . \tag{16}$$

This action induces a right-action of $\mathrm{End}(V)$ on V^n.

The reference basis induces an isomorphism $\mathrm{End}(V) \simeq \mathcal{M}_2(\mathbb{R})$. Let $v \in V$ with expression $(v_1\ v_2)$ in the reference basis. A matrix $M \in \mathcal{M}_2(\mathbb{R})$ acts on V as:

$$v \cdot M = (v_1\ v_2) \cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix} = (av_1 + cv_2\ bv_1 + dv_2) \ . \tag{17}$$

Definition 18. *As usual,* $\det : \mathrm{End}(V) \to \mathbb{R}$ *is the unique map which satisfies*

$$(v^1 \cdot A) \wedge (v^2 \cdot A) = \det(A) \cdot (v^1 \wedge v^2)$$

for $A \in \mathrm{End}(V)$ and $v^1, v^2 \in V$. Let us also set:

$$\begin{aligned} \mathrm{GL}(V) &= \det^{-1}(\mathbb{R}^*) \\ \mathrm{SL}(V) &= \det^{-1}(\{1\}) \\ \mathrm{GL}^+(V) &= \det^{-1}(\mathbb{R}_+^*) \ . \end{aligned}$$

Remark 7. *The reference basis induces the isomorphism:*

$$\begin{array}{ccc} \mathcal{B}^+ & \to & \mathrm{GL}_2^+(\mathbb{R}) \\ \begin{pmatrix} f^1 \\ f^2 \end{pmatrix} & \mapsto & \begin{pmatrix} f_1^1 & f_2^1 \\ f_1^2 & f_2^2 \end{pmatrix} \end{array} \tag{18}$$

where f_1^i and f_2^i are the coordinates of f^i in the reference basis ($i = 1, 2$).

Let $(v_1\ v_2)_{\mathcal{B}}$ be the expression of v in coordinates, in a basis $\mathcal{B}$. Then $(v_1, v_2)_{\mathcal{B}} \cdot M^{-1}$ is the expression in coordinates of the same vector, but in the basis $M \cdot \mathcal{B}$.

A.2 Lattices

Definition 19. *A lattice L in V is an additive subgroup of V isomorphic to $\mathbb{Z}^2$ as a $\mathbb{Z}$-module, and such that*

$$L \otimes_{\mathbb{Z}} \mathbb{R} = V \ .$$

Let $\mathcal{L}$ be the set of all lattices in V.

There is a natural surjection:

$$\begin{array}{ccc} \mathcal{B}^+ & \to & \mathcal{L} \\ (v^1, v^2) & \mapsto & \mathbb{Z}v^1 + \mathbb{Z}v^2 \end{array} \ . \tag{19}$$

The set (v^1, v^2) is a basis of $L = \mathbb{Z}v^1 + \mathbb{Z}v^2$ as a free $\mathbb{Z}$-module.

Proposition 23. *Two oriented bases*

$$\begin{pmatrix} v^1 \\ v^2 \end{pmatrix} = \begin{pmatrix} v_1^1 & v_2^1 \\ v_1^2 & v_2^2 \end{pmatrix} \text{ and } \begin{pmatrix} w^1 \\ w^2 \end{pmatrix} = \begin{pmatrix} w_1^1 & w_2^1 \\ w_1^2 & w_2^2 \end{pmatrix}$$

project to the same lattice if the two matrices are related by left-multiplication by an element of $\mathrm{SL}_2(\mathbb{Z})$.

Proof. Let us assume that:

$$\mathbb{Z}v^1 + \mathbb{Z}v^2 = \mathbb{Z}w^1 + \mathbb{Z}w^2 \ .$$

Then, there exist $m_j^i \in \mathbb{Z}$ and $n_j^i \in \mathbb{Z}$, $i, j = 1, 2$, such that for all $j = 1, 2$, one has

$$\begin{aligned} w^j &= m_1^j v^1 + m_2^j v^2 \\ v^j &= n_1^j w^1 + n_2^j w^2 \end{aligned}$$

The matrices $M = (m_j^i)$ and $N = (n_j^i)$ are by construction mutually inverse. □

In other words:

$$\mathcal{L} \simeq \mathrm{SL}_2(\mathbb{Z}) \backslash \mathrm{GL}_2^+(\mathbb{R}) \ . \tag{20}$$

Let $L_1^{np} \in \mathcal{L}$ be the **(non-projective) reference lattice**, defined as

$$L_1^{np} = \mathbb{Z}e^1 + \mathbb{Z}e^2 \ . \tag{21}$$

A.3 Projective lattices

The embedding

$$\begin{array}{ccc} \mathbb{R}^\times & \to & \mathrm{GL}_2^+(\mathbb{R}) \\ \alpha & \mapsto & \begin{pmatrix} \alpha & 0 \\ 0 & \alpha \end{pmatrix} \end{array} \tag{22}$$

is central, hence there is a well defined left-action of $\mathbb{R}^\times$ on $\mathcal{L}$ given by:

$$\alpha \cdot (\mathrm{SL}_2(\mathbb{Z}) \cdot (v_1, v_2)) = \mathrm{SL}_2(\mathbb{Z}) \cdot (\alpha v_1, \alpha v_2) \ . \tag{23}$$

Definition 20. *Let $\mathrm{P}\mathcal{L} = \mathbb{R}^\times \backslash \mathcal{L}$ be the set of projective lattices in V. By definition, a projective lattice is an equivalence class of lattices which are scalar multiples of each other.*

Let also $\mathrm{P}\mathcal{B}^+$ be the set of projective oriented bases in V, that is, $\mathrm{P}\mathcal{B}^+ = \mathbb{R}^\times \backslash \mathcal{B}^+$. Hence $\mathrm{P}\mathcal{L} \simeq \mathrm{PSL}_2(\mathbb{Z}) \backslash \mathrm{P}\mathcal{B}^+$, where $\mathrm{PSL}_2(\mathbb{Z}) = \{\pm 1\} \backslash \mathrm{SL}_2(\mathbb{Z})$. Once again, the reference basis in V induces an isomorphism:

$$\mathrm{P}\mathcal{L} \simeq \mathrm{PSL}_2(\mathbb{Z}) \backslash \mathrm{PGL}_2^+(\mathbb{R}) \ . \tag{24}$$

Example 9. *The projective lattice corresponding to the coset*

$$\mathrm{PSL}_2(\mathbb{Z}) \cdot \begin{bmatrix} f_1^1 & f_2^1 \\ f_1^2 & f_2^2 \end{bmatrix}$$

is the projective class containing the lattice generated by the vectors $f^1 = (f_1^1 \ f_2^1)$ and $f^2 = (f_1^2 \ f_2^2)$, where the coordinates are the ones in the reference basis.

A.4 Commensurable lattices

Definition 21. *A (non-projective) lattice $L^{np} \in \mathcal{L}$ is said to be* **commensurable** *with L_1^{np} if the intersection $L^{np} \cap L_1^{np}$ has finite index in both L^{np} and L_1^{np}.*

Consider the two-dimensional $\mathbb{Q}$-vector space

$$V_1 = L_1^{np} \otimes_{\mathbb{Z}} \mathbb{Q} \subset V \ . \tag{25}$$

It satisfies $V_1 \otimes_{\mathbb{Q}} \mathbb{R} = V$.

Remark 8. *The lattices in V which are commensurable with L_1^{np} correspond exactly to the additive subgroups of V_1 isomorphic to $\mathbb{Z}^2$ as $\mathbb{Z}$-modules.*

Let $\mathcal{B}_1^+$ be the set of oriented bases of V_1, and let

$$\mathcal{L}_1 := \mathrm{SL}_2(\mathbb{Z}) \backslash \mathcal{B}_1^+ \ , \tag{26}$$

By Remark 8, $\mathcal{L}_1$ is the subset of $\mathcal{L}$ which contains the lattices in V commensurable with L_1^{np}. The reference basis induces the isomorphism

$$\mathcal{L}_1 \simeq \mathrm{SL}_2(\mathbb{Z}) \backslash \mathrm{GL}_2^+(\mathbb{Q}) \ . \tag{27}$$

Let the rational projectivisation of the set of lattices commensurable with L_1^{np} be the set of rationally projective lattices such that one (equivalently, all) of their representatives is commensurable with L_1^{np}:

$$\mathrm{P}\mathcal{L}_1 = \mathbb{Q}^\times\backslash\mathcal{L}_1 \simeq \mathrm{PSL}_2(\mathbb{Z})\backslash\mathrm{P}\mathcal{B}_1^+ \ ,$$

where $\mathrm{P}\mathcal{B}_1^+ = \mathbb{Q}^\times\backslash\mathcal{B}_1^+$. The reference basis again induces:

$$\mathrm{P}\mathcal{L}_1 \simeq \mathrm{PSL}_2(\mathbb{Z})\backslash\mathrm{PGL}_2^+(\mathbb{Q}) \ . \tag{28}$$

The rational projectivisation of L_1^{np} is denoted L_1 and called the reference projective lattice, or **reference lattice**, for short. We drop the P (standing for projective) in L_1 in order to keep the notation as light as possible. Hopefully, the superscript on L_1^{np} which emphasizes the non-projective nature of the latter will help keeping things clear.

A.5 Hyperdistance on $\mathrm{P}\mathcal{L}_1$

Let $M = (m_i^j)$ be a non-zero 2×2 matrix with rational coefficients. There exists a smallest strictly positive rational number α_M such that

$$\forall i, j \in \{1, 2\},\ \alpha_M m_i^j \in \mathbb{Z} \ .$$

Let us consider the map

$$\begin{array}{rcl} \mathrm{Pdet} : \mathcal{M}_2(\mathbb{Q}) & \to & \mathbb{Z} \\ M & \mapsto & \det(\alpha_M M) = \alpha_M^2 \det(M) \end{array} \ . \tag{29}$$

For all $x \in \mathbb{Q}^\times$ one has $\det(xM) = \det(M)$, hence this map is well defined on the rational projective space $\mathrm{P}\mathcal{M}_2(\mathbb{Q})$.

Proposition 24. *Let $A \in \mathrm{SL}_2(\mathbb{Z})$. Then for all $X \in \mathcal{M}_2(\mathbb{Q})$, one has:*

$$\mathrm{Pdet}([AX]) = \mathrm{Pdet}([X]) = \mathrm{Pdet}([XA])$$

where $[X]$ denotes the rational projective class of X.

Proof. It suffices to show that $\alpha_{AX} = \alpha_X = \alpha_{XA}$. Since A and A^{-1} have integer entries, αAX has integer entries if and only if αX has integer entries, hence

$$\{\alpha | \alpha X \in \mathcal{M}_2(\mathbb{Z})\} = \{\alpha | \alpha AX \in \mathcal{M}_2(\mathbb{Z})\} \ ,$$

and they have the same minimal element. □

Definition 22. *The projective determinant (still denoted* Pdet*) is the (induced) function*

$$\mathrm{Pdet} : \mathrm{PSL}_2(\mathbb{Z})\backslash\mathrm{PGL}_2^+(\mathbb{Q}) \to \mathbb{N}_{>0} \ .$$

It is invariant under the right-action of $\mathrm{PSL}_2(\mathbb{Z})$.

Let $L, L' \in \mathrm{P}\mathcal{L}_1$, and let M, M' be representatives in $\mathrm{GL}_2^+(\mathbb{Q})$ of the corresponding elements in $\mathrm{PSL}_2(\mathbb{Z})\backslash\mathrm{PGL}_2^+(\mathbb{Q})$. Set:

$$\delta(L, L') = \mathrm{Pdet}(M(M')^{-1}) \ . \tag{30}$$

Proposition 25. *The function*

$$\delta : \mathrm{P}\mathcal{L}_1 \times \mathrm{P}\mathcal{L}_1 \to \mathbb{N}_{>0}$$

is symmetric. It is called **hyperdistance**.

Proof. Let $M \in \mathcal{M}_2(\mathbb{Z})$ be invertible as a rational matrix. Then, $\det(M)M^{-1} \in \mathcal{M}_2(\mathbb{Z})$. Replacing M in $\det(M)M^{-1}$ with $\det(M)M^{-1}$ implies that if $\det(M)M^{-1}$ is an invertible rational matrix with integer entries, $\det\left(\det(M)M^{-1}\right)\left(\det(M)M^{-1}\right)^{-1} = M \in \mathcal{M}_2(\mathbb{Z})$.

Thus a 2×2 invertible rational matrix M has integer entries if and only if $\det(M)M^{-1}$ does, and hence $\alpha_M M$ has integer entries if and only if $\alpha_M \det(M)M^{-1}$ does. This implies:

$$\alpha_{M^{-1}} = \alpha_M \det(M) \ .$$

As a consequence of this last equality, one has $\mathrm{Pdet}(M) = \mathrm{Pdet}(M^{-1})$, which proves the claim. □

Remark 9. *The logarithm of the (judiciously named) hyperdistance is a metric on* $\mathrm{P}\mathcal{L}_1$ *(see [Con96]). Note that in dimension strictly greater than* 2*, the function analogous to* δ *is not symmetric anymore.*

Let $N \in \mathbb{N}_{>0}$. The set of projective lattices N-hyperdistant from L_1 is the set

$$\mathrm{P}\mathcal{L}_1^N = \{L \in \mathrm{P}\mathcal{L}_1 | \delta(L, L_1) = N\} \ . \tag{31}$$

This particular subset of $\mathrm{P}\mathcal{L}_1$ can be characterised as follows. Let $\tilde{L}^{np}$ be any representative of some $L \in \mathrm{P}\mathcal{L}_1$ such that $\tilde{L}^{np}$ is a subgroup of L_1^{np}. The index of $\tilde{L}^{np}$ in L_1^{np} is as usual the order of the finite cyclic abelian group $\tilde{L}^{np}\backslash L_1^{np}$. Then, $\mathrm{P}\mathcal{L}_1^N$ consists of the projective lattices in $\mathrm{P}\mathcal{L}_1$ such that among all their representatives which are subgroups of L_1^{np}, the minimum of the index function is N.

For exemple, consider any sublattice $\tilde{L}^{np}$ of index 2 in L_1^{np}. Since 2 is prime, the projective class of $\tilde{L}^{np}$ is always 2-hyperdistant from L_1. However, the representative $2 \cdot \tilde{L}^{np}$ of the same projective lattice is of index 8 ($= 2 \times 2^2$) in L_1^{np}.

A.6 Elements of $\mathrm{P}\mathcal{L}_1$

Let us describe and label the elements of $\mathrm{P}\mathcal{L}_1 = \mathrm{PSL}_2(\mathbb{Z})\backslash\mathrm{PGL}_2^+(\mathbb{Q})$ as in [Con96]. Consider the map

$$\mathrm{GL}_2^+(\mathbb{Q}) \to \mathrm{PSL}_2(\mathbb{Z})\backslash\mathrm{PGL}_2^+(\mathbb{Q}) \ . \tag{32}$$

For each coset $\mathrm{PSL}_2(\mathbb{Z})\cdot g$ in its image, let $g = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{PGL}_2^+(\mathbb{Q})$ denote the projective class of the matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2^+(\mathbb{Q})$.

Let $s, t \in \mathbb{Z}$ be such that $sa + tc = 0$, with s and t relatively prime. Since the columns of g are linearly independent, it must be that $sb + td \neq 0$. Since s and t have no common factor, there exist $m, n \in \mathbb{Z}$ such that $mt - sn = 1$. In other words, there exists $H \in \mathrm{PSL}_2(\mathbb{Z})$ such that:

$$H \cdot g = \begin{bmatrix} m & n \\ s & t \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} a' & b' \\ 0 & d' \end{bmatrix} = g' \ ,$$

with $b' \in \mathbb{Q}$ and $a', d' \in \mathbb{Q}^\times$. Moreover, $\begin{bmatrix} a' & b' \\ 0 & d' \end{bmatrix} = \begin{bmatrix} a'' & b'' \\ 0 & 1 \end{bmatrix}$ with $a'' = a'/d'$ and $b'' = b'/d'$. Let N be the unique integer such that $0 \leq b'' + N < 1$. Then, left-multiplication of the latter element of $\mathrm{PGL}_2^+(\mathbb{Q})$ by $\begin{bmatrix} 1 & N \\ 0 & 1 \end{bmatrix} \in \mathrm{PSL}_2(\mathbb{Z})$ yields some $\begin{bmatrix} M & b \\ 0 & 1 \end{bmatrix}$. Furthermore, the only element in $\mathrm{PSL}_2(\mathbb{Z})$ which maps representatives of projective classes of this form to representatives of the same form is easily shown to be the identity. Hence we have proved the following

Proposition 26. *Let $\mathcal{M}$ be the set of matrices of the form $\begin{pmatrix} M & b \\ 0 & 1 \end{pmatrix}$ with $M \in \mathbb{Q}_+^*$ and $b \in \mathbb{Q} \cap [0, 1[$. Then*

$$\begin{array}{rcl} \mathcal{M} & \to & \mathrm{PSL}_2(\mathbb{Z}) \backslash \mathrm{PGL}_2^+(\mathbb{Q}) \\ \begin{pmatrix} M & b \\ 0 & 1 \end{pmatrix} & \mapsto & \mathrm{PSL}_2(\mathbb{Z}) \cdot \begin{bmatrix} M & b \\ 0 & 1 \end{bmatrix} \end{array}$$

is a bijection.

Definition 23. *Let $g_{M,b}$ denote the coset*

$$\mathrm{PSL}_2(\mathbb{Z}) \cdot \begin{bmatrix} M & b \\ 0 & 1 \end{bmatrix} \in \mathrm{PSL}_2(\mathbb{Z}) \backslash \mathrm{PGL}_2^+(\mathbb{Q}) \ .$$

Let $L_{M,b} := \mathrm{PSL}_2(\mathbb{Z}) \cdot g_{M,b}$ be the projective lattice corresponding to the class of $g_{M,b}$. We always shorten $g_{M,0}$ and $L_{M,0}$ to g_M and L_M.

Note that this definition of L_1 coincides with the first one we considered.

Corollary 5. *This classification of the cosets in $\mathrm{PSL}_2(\mathbb{Z}) \backslash \mathrm{PGL}_2^+(\mathbb{Q})$ implies that any projective lattice commensurable with L_1 has a unique non-projective representative with basis of the form*

$$f^1 = (M \ b), \ f^2 = (0 \ 1) \ ,$$

where $M \in \mathbb{Q}_+^*$ and $b \in \mathbb{Q} \cap [0, 1[$.

Example 10. *The projective lattice L_N corresponds to the coset $\mathrm{PSL}_2(\mathbb{Z}) \cdot \begin{bmatrix} N & 0 \\ 0 & 1 \end{bmatrix}$, and hence to the class of non-projective lattices $\{\mathbb{Z} \cdot (\alpha N \ 0) + \mathbb{Z} \cdot (0 \ \alpha) | \ \alpha \in \mathbb{Q}^\times\}$.*

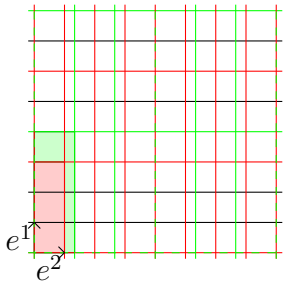


Figure 25: Two non-projective representatives of L_3 (in green and red) on L_1^{np}.

A.7 Stabilisers and Hecke Congruence Subgroups of $\mathrm{PSL}_2(\mathbb{Z})$

Let $G := \mathrm{PGL}_2^+(\mathbb{Q})$ and consider its right-action on $\mathrm{P}\mathcal{L}_1$

$$\begin{bmatrix} f_1^1 & f_2^1 \\ f_1^2 & f_2^2 \end{bmatrix} . \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} af_1^1 + cf_2^1 & bf_1^1 + df_2^1 \\ af_1^2 + cf_2^2 & bf_1^2 + df_2^2 \end{bmatrix} . \tag{33}$$

Let $G_L := \mathrm{Fix}_G(L)$ be the stabiliser of $L \in \mathrm{P}\mathcal{L}_1$ in G. The group G_{L_1} is easily shown to be $\mathrm{PSL}_2(\mathbb{Z})$. This is the definition of the modular group we were aiming for. Now, since G acts transitively on $\mathrm{P}\mathcal{L}_1$, the stabiliser of any $L \in \mathrm{P}\mathcal{L}_1$ is a conjugate of G_1 in $\mathrm{PGL}_2^+(\mathbb{Q})$. For example, and for $M \in \mathbb{Q}_+^*$, one has

$$G_M = g_M^{-1} G_1 g_M = \left\{ \begin{bmatrix} a & b/M \\ cM & d \end{bmatrix} \mid a, b, c, d \in \mathbb{Z},\ ad - bc = 1 \right\} . \tag{34}$$

Subsequently, the subgroup of G which stabilizes the pair (L_1, L_N) is $G_{(L_1,L_N)} = G_1 \cap G_N$. For $N \in \mathbb{N}_{>0}$ one has:

$$G_{(L_1,L_N)} = \left\{ \begin{bmatrix} a & b \\ cN & d \end{bmatrix} \mid a, b, c, d \in \mathbb{Z},\ ad - bcN = 1 \right\} . \tag{35}$$

Definition 24. *Let N be a positive integer. The* **Hecke congruence subgroup** *of level N of the modular group is the group*

$$\Gamma_0(N) := \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \mid a, b, c, d \in \mathbb{Z},\ ad - bc = 1,\ c \equiv 0[N] \right\} < \mathrm{PSL}_2(\mathbb{Z}) .$$

Note that $\Gamma_0(1) = \mathrm{PSL}_2(\mathbb{Z})$.

References

[AL70] A.O.L. Atkin and J. Lehner. Hecke operators on Γ0(m). *Mathematische Annalen*, 185(2):134–160, jun 1970.

[Bel80] G.V. Belyĭ. On galois extensions of a maximal cyclotomic field. *Mathematics of the USSR - Izvestija*, 14(2):247–256, apr 1980.

[Bor92] R.E. Borcherds. Monstrous moonshine and monstrous lie superalgebras. *Invent. Math.*, 109(2):405–444, 1992.

[CCN+03] J.H. Conway, R.T. Curtis, S.P. Norton, R.A. Parker, and R.A. Wilson. *ATLAS of Finite Groups*. OUP, 2003.

[CN79] J.H. Conway and S.P. Norton. Monstrous moonshine. *Bull. London Math. Soc.*, 11(3):308–339, 1979.

[Con85] J.H. Conway. A simple construction for the Fischer-Griess monster group. *Inventiones Mathematicae*, 79:513–540, 1985.

[Con96] J.H. Conway. Understanding groups like $\Gamma_0(N)$. *Ohio State Univ. Math. Res. Inst. Publ.*, 4(3):327–343, 1996.

[CWZ00] J.A. Csirik, J.L. Wetherell, and M.E. Zieve. On the genera of x_0 (n). *arXiv preprint math/0006096*, 2000.

[DGO15] J.F. Duncan, M.J. Griffin, and K. Ono. Moonshine. *Research in the Mathematical Sciences*, 2:11, 2015.

[Dun09] J.F. Duncan. Arithmetic groups and the affine E_8 Dynkin diagram. In *Groups and Symmetries: From Neolithic Scots to John McKay*, volume 47 of *CRM Proceedings and Lecture Notes*, pages 135–163, Providence, RI, 2009. Amer. Math. Soc.

[FLM89] I. Frenkel, J. Lepowsky, and A. Meurman. *Vertex operator algebras and the Monster*. Academic press, 1989.

[Ful89] W. Fulton. *Algebraic curves: an introduction to algebraic geometry*. Addison-Wesley, 1989.

[Gan06] T. Gannon. *Moonshine beyond the Monster: The bridge connecting algebra, modular forms and physics*. Cambridge University Press, 2006.

[Gro13] A. Grothendieck. Esquisse d'un programme. In *Geometric Galois Actions*, pages 7–48. Cambridge University Press, apr 2013.

[HM15] Y.-H. He and J. McKay. Sporadic and Exceptional. *arXiv preprint*, pages 1–49, 2015.

[JW16] G.A. Jones and J. Wolfart. *Dessins d'enfants on Riemann Surfaces*. Springer, 2016.

[Man72] J.I. Manin. PARABOLIC POINTS AND ZETA-FUNCTIONS OF MODULAR CURVES. *Mathematics of the USSR-Izvestiya*, 6(1):19–64, 1972.

[Mil97] J.S. Milne. Modular functions and modular forms. *University of Michigan lecture notes*, 1997. `https://www.jmilne.org/math/CourseNotes/mf.html`.

[Pla19] J. Plazas. Noncommutative geometry of groups like $\Gamma_0(N)$. *p-Adic Numbers, Ultrametric Anal. Appl.*, 11(1):61–76, jan 2019.

[S+18] W.A. Stein et al. *Sage Mathematics Software*. The Sage Development Team, 2018. `http://www.sagemath.org`.

[Sch94] L. Schneps. *The Grothendieck Theory of Dessins d'Enfants*. Cambridge University Press, jul 1994.

[Sch11] L. Schneps. Dessins d'enfants on the Riemann sphere. In *The Grothendieck Theory of Dessins d'Enfants*, pages 47–78. Cambridge University Press, jul 2011.

[Shi71] G. Shimura. *Introduction to the Arithmetic Theory of Automorphic Functions*. Kanô memorial lectures. Princeton University Press, 1971.

[Smi85] S.D. Smith. On the head characters of the monster simple group. *Contemp. Math.*, 45:303–313, 1985.

[Tho79] J. G. Thompson. Some Numerology between the Fischer-Griess Monster and the Elliptic Modular Function. *Bulletin of the London Mathematical Society*, 11(3):352–353, 10 1979.

[VH] M. Van Hoeij. Parametrization of the modular curve $X_0(N)$ for n from 2 to 37. `https://www.math.fsu.edu/~hoeij/files/X0N/Parametrization`. Accessed: 2020-07-08.